Simatic Tip

SIMATIC TIPS

Totally Integrated Automation
Application Notes

Group
PLC Scalance

Topic and Author
Configuration of M875 with IPsec VPN Tunnel Bernd Krueger

Overview

This document covers how to configure the M875 for connection to a PLC using a VPN Tunnel using the Siemens SoftNet Client Software. It is assumed that the user is already proficient in the use of Siemens PLCs, Step 7 V5.5 and/or the TIA Portal software.

As a cautionary note: Siemens takes no responsibility for any data overage or roaming charges for any services used with the M875 device. Always review your data plan before configuring and using this device so that you are aware of proper configuration for you usage plan.

STEP by STEP

Step 1 thru 26 – M875 Configuration

Step 27– PLC Configuration

Step 28 thru 75 – VPN Configuration

Resetting the M875 to Factory Defaults

To reset the M875, press the Reset button on the front of the unit with a paperclip. This will take a few minutes and the lights on the device will begin to flash. All configuration data, user data, certificates and log files are deleted.

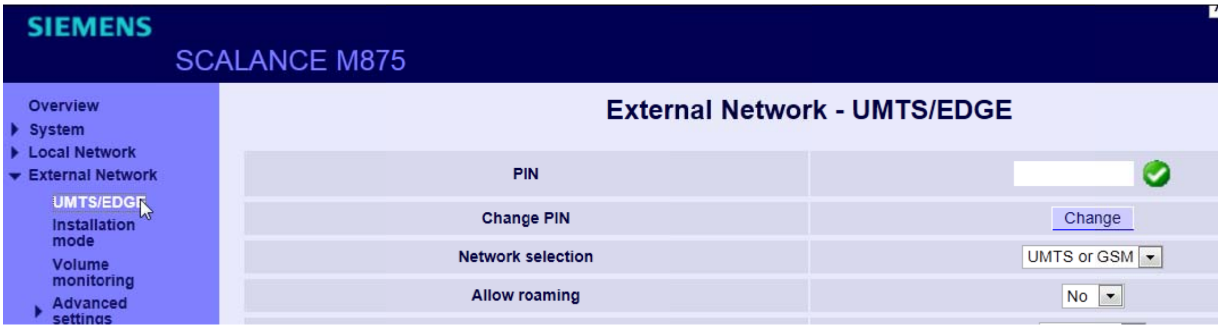
Step 1 – Acquire AT&T data plan

If you have an existing Corporate AT&T account contact your designated person. If you do not already have a corporate AT&T account please contact your local Siemens person. As of the writing of this Application Note that person is: Ming Ng, email is daming.ng@siemens.com and he can put you in contact the correct AT&T representative. Sim cards can be ordered with or without Static IP addresses. Before you commit to a plan always check your coverage, for ATT you can go to www.att.com/coverage. You can also get coverage apps for your mobile phone for example www.mymobilecoverage.com. One more note ATT Wireless Hotspots will not work with the M875 due to their policy of blocking mobile to mobile communication.

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 2 – Enter PIN number if required – not normal in USA

In the USA it is normally not required to enter a PIN number for a sim card, but if required follow steps 4 thru 6 below. DO NOT PUT THE SIM CARD IN THE M875 IF YOU REQUIRE A PIN. Then go to “External Network” “UMTS/EDGE”, enter the PIN number and save. After saving Power Off the M875 and continue to Step 3.

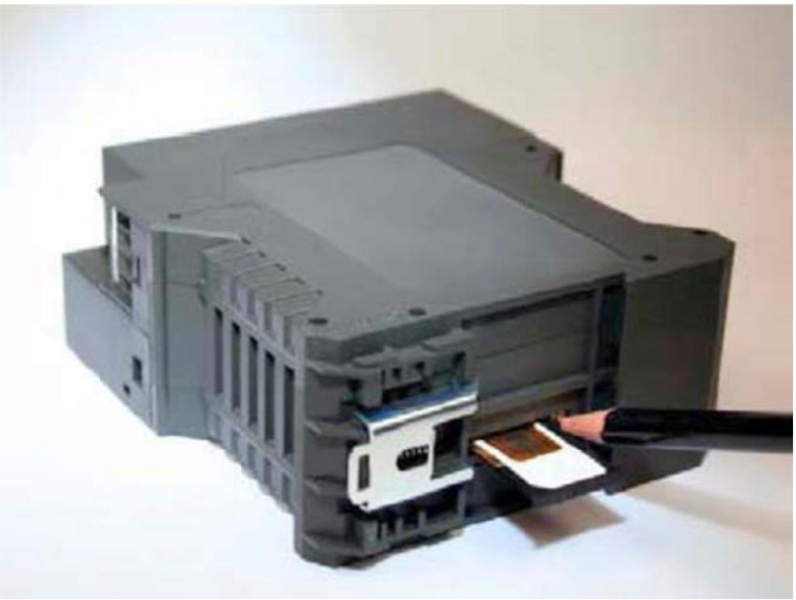


External Network - UMTS/EDGE

PIN	
Change PIN	Change
Network selection	UMTS or GSM
Allow roaming	No

Step 3 – Insert SIM card

- Before you insert or remove the SIM card, turn off the power supply of the M875. Do not open the compartment for the SIM card during operation. This can damage the SIM card and the device.
- The compartment for the SIM card is located on the back of the device.
- To open the drawer, press the yellow button with a sharp object, for example a pencil.
- Place the SIM card in the tray so that the card audibly locks in place and so that its goldplated contacts remain visible.
- Then push the tray with the SIM card completely back into the housing



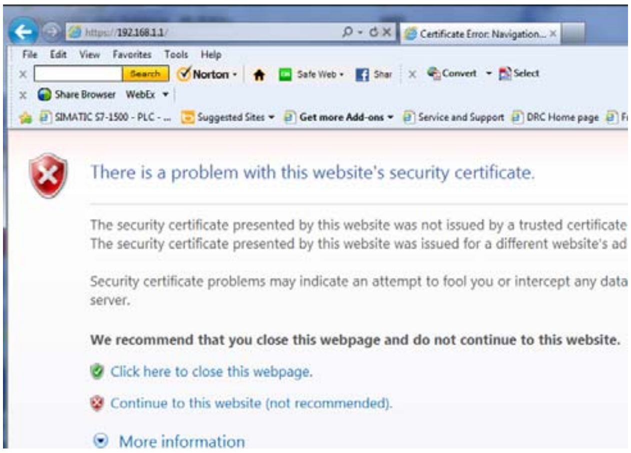
Step 4 – Configuration PC

The configuration PC must be connected either directly to the first Ethernet port of the M875 or have access to the M875 via the local network. The network adapter of the configuration PC must have the following TCP/IP configuration:

- IP address: 192.168.1.x – x being any number other than 1.
- Subnet mask: 255.255.255.0

Step 5 – Connect using “Internet Explorer” or “Mozilla Firefox”

Enter the M875’s IP address – the default is: https://192.168.1.1



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate
The security certificate presented by this website was issued for a different website's ad

Security certificate problems may indicate an attempt to fool you or intercept any data server.

We recommend that you close this webpage and do not continue to this website.

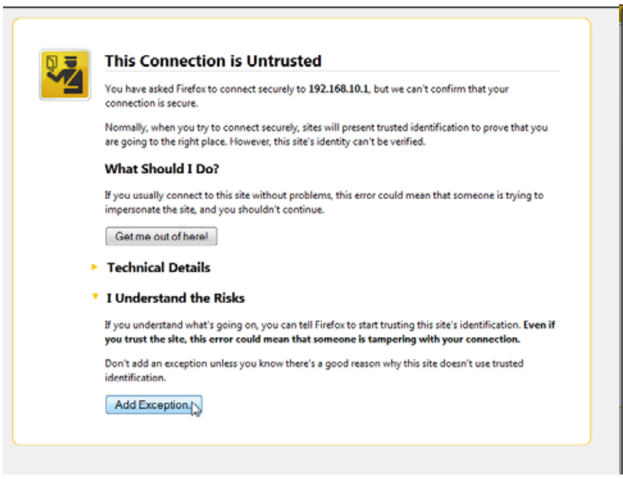
Click here to close this webpage.

Continue to this website (not recommended).

More information

In “Internet Explorer select the “Red X” Continue to this website.

For Mozilla Firefox:



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.10.1**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

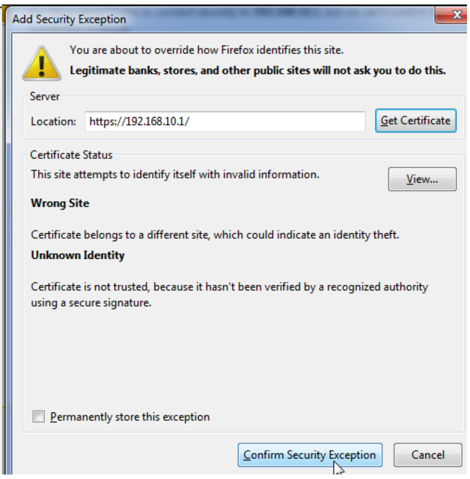
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.



Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server
Location: https://192.168.10.1/

Certificate Status
This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

Unknown Identity

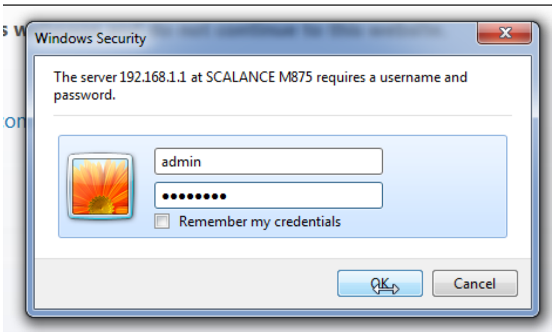
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☐ Permanently store this exception

Select “Add Exceptions”

Either uncheck or leave checked “Permanently store this exception” and then press “Confirm Security Exception”.

Step 6 – Enter Login data



Windows Security

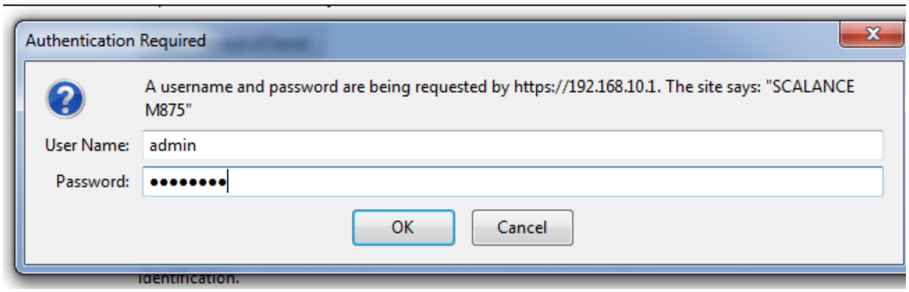
The server 192.168.1.1 at SCALANCE M875 requires a username and password.

admin

••••••••

□ Remember my credentials

Internet Explorer login screen – enter “admin” and “scalance” for first time login.



Authentication Required

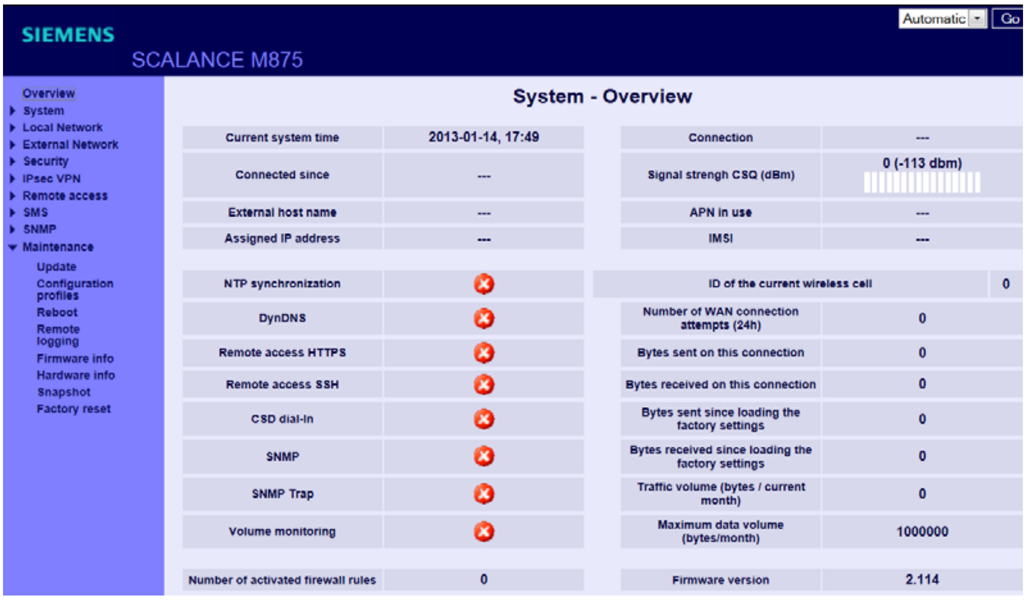
A username and password are being requested by https://192.168.10.1. The site says: "SCALANCE M875"

User Name: admin

Password: ••••••••

Mozilla Firefox login screen – enter “admin” and “scalance” for first time login.

Step 7 – Overview Screen at startup



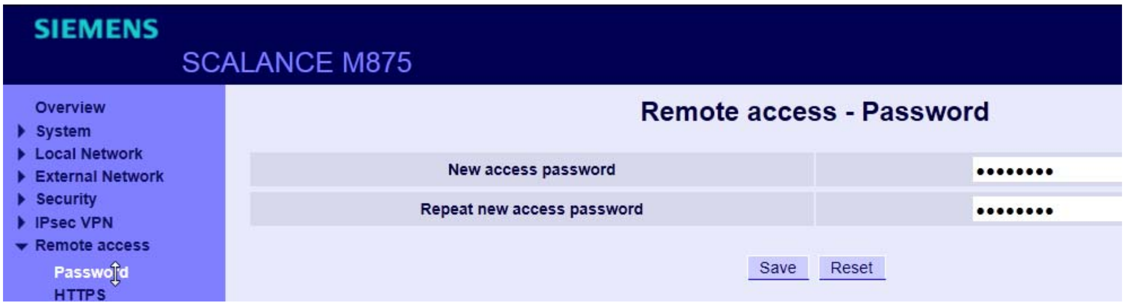
System - Overview

Current system time	2013-01-14, 17:49	Connection	---
Connected since	---	Signal strengh CSQ (dBm)	0 (-113 dbm)
External host name	---	APN in use	---
Assigned IP address	---	IMSI	---
NTP synchronization	☒	ID of the current wireless cell	0
DynDNS	☒	Number of WAN connection attempts (24h)	0
Remote access HTTPS	☒	Bytes sent on this connection	0
Remote access SSH	☒	Bytes received on this connection	0
CSD dial-In	☒	Bytes sent since loading the factory settings	0
SNMP	☒	Bytes received since loading the factory settings	0
SNMP Trap	☒	Traffic volume (bytes / current month)	0
Volume monitoring	☒	Maximum data volume (bytes/month)	1000000
Number of activated firewall rules	0	Firmware version	2.114

After logging into the system the “Overview” screen is shown.

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 8 – Change Default Password



Remote access - Password

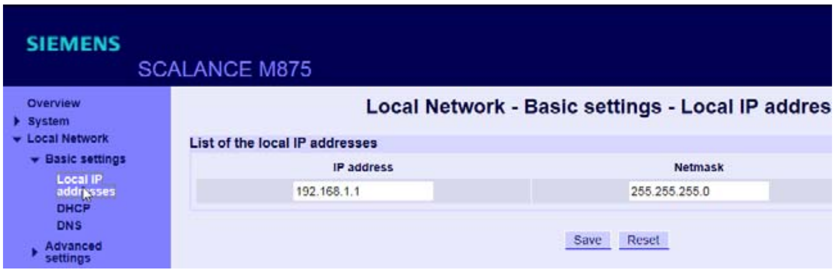
New access password	••••••••
Repeat new access password	••••••••

For security reasons it is highly recommended to immediately change from the Default password. To do this go to the “Remote access” “Password” tab on the left hand side of the screen. For a secure password do not use something that is in the dictionary, at lease 8 characters long and include “Upper case, lower case, numbers, and special characters”. The following special characters are allowed:

! $ % & ’ ( ) * + , . / : ; < = > ? @ [¥] ^ _ ` { | }

After entering the new password press “Save”, you will then be requested to log back into the M875.

Step 9 – View default IP address



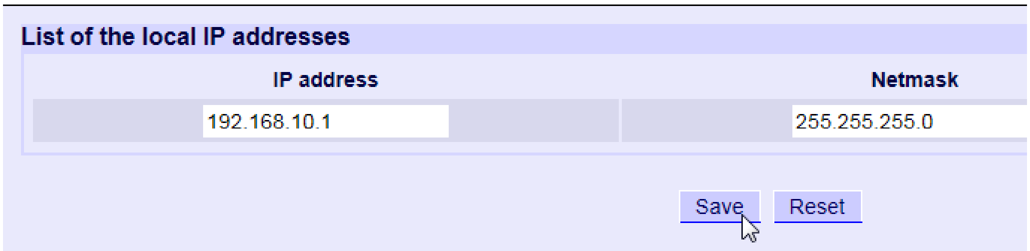
Local Network - Basic settings - Local IP addres

List of the local IP addresses

IP address	Netmask
192.168.1.1	255.255.255.0

Go to the “Local IP addresses” as shown in the picture.

Step 10 – Change default IP address



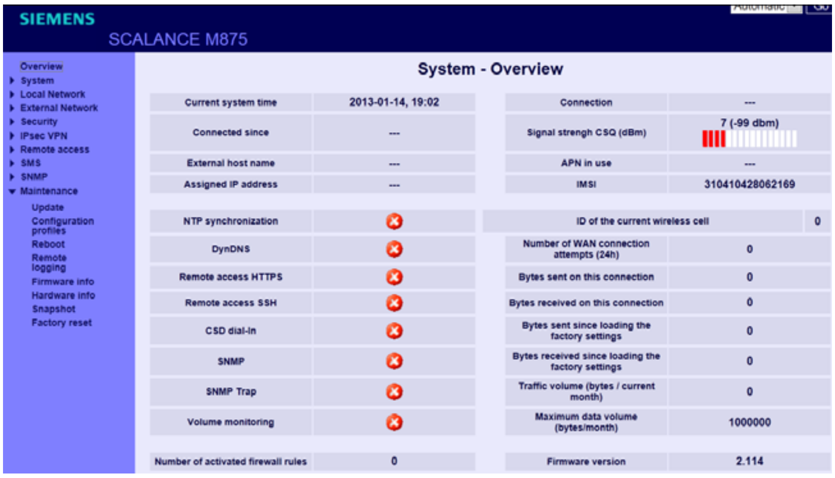
List of the local IP addresses

IP address	Netmask
192.168.10.1	255.255.255.0

For our project we need to use a 192.168.10.x IP address range. Change the address of the M875 to 192.168.10.1 and 255.255.255.0 and then press “Save”. Change the IP address of your computer to something in 192.168.10.x range (192.168.10.99 for example). In “Internet Explorer” or “Mozilla Firefox” change the site to connect to https://192.168.10.1 and log back in using your new password.

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 11 – Overview Screen

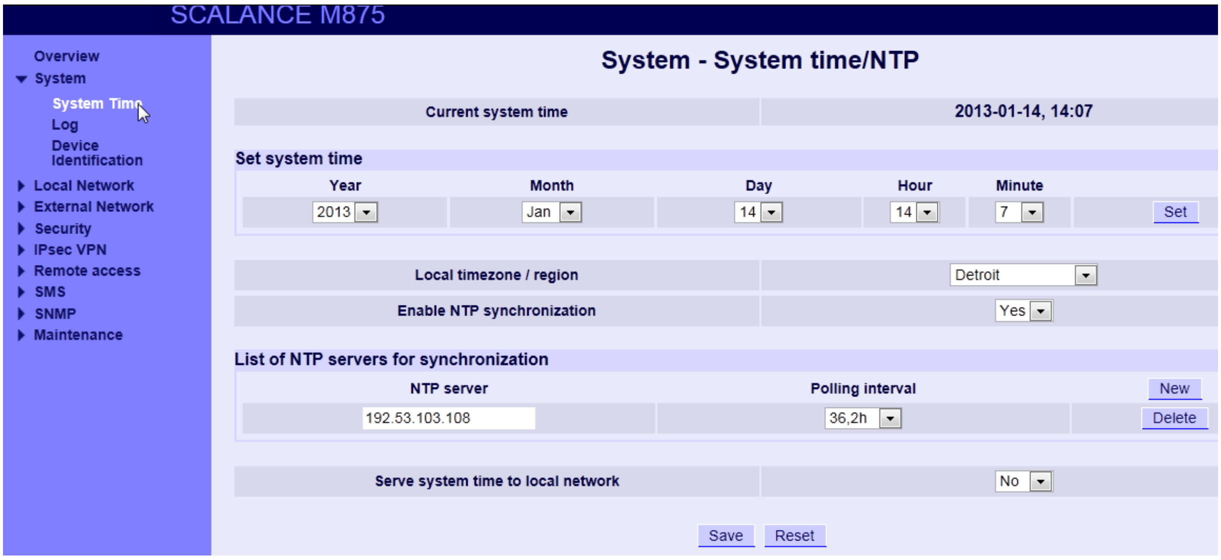


System - Overview

Current system time	2013-01-14, 19:02	Connection	---
Connected since	---	Signal strengh CSQ (dBm)	7 (-99 dbm)
External host name	---	APN in use	---
Assigned IP address	---	IMSI	310410428062169
NTP synchronization	✗	ID of the current wireless cell	0
DynDNS	✗	Number of WAN connection attempts (24h)	0
Remote access HTTPS	✗	Bytes sent on this connection	0
Remote access SSH	✗	Bytes received on this connection	0
CSD dial-In	✗	Bytes sent since loading the factory settings	0
SNMP	✗	Bytes received since loading the factory settings	0
SNMP Trap	✗	Traffic volume (bytes / current month)	0
Volume monitoring	✗	Maximum data volume (bytes/month)	1000000
Number of activated firewall rules	0	Firmware version	2.114

With the SIM card inserted you will see a screen similar to this.

Step 12 – Set the system time



System - System time/NTP

Current system time: 2013-01-14, 14:07

Set system time

Year	Month	Day	Hour	Minute
2013	Jan	14	14	7

Local timezone / region: Detroit

Enable NTP synchronization: Yes

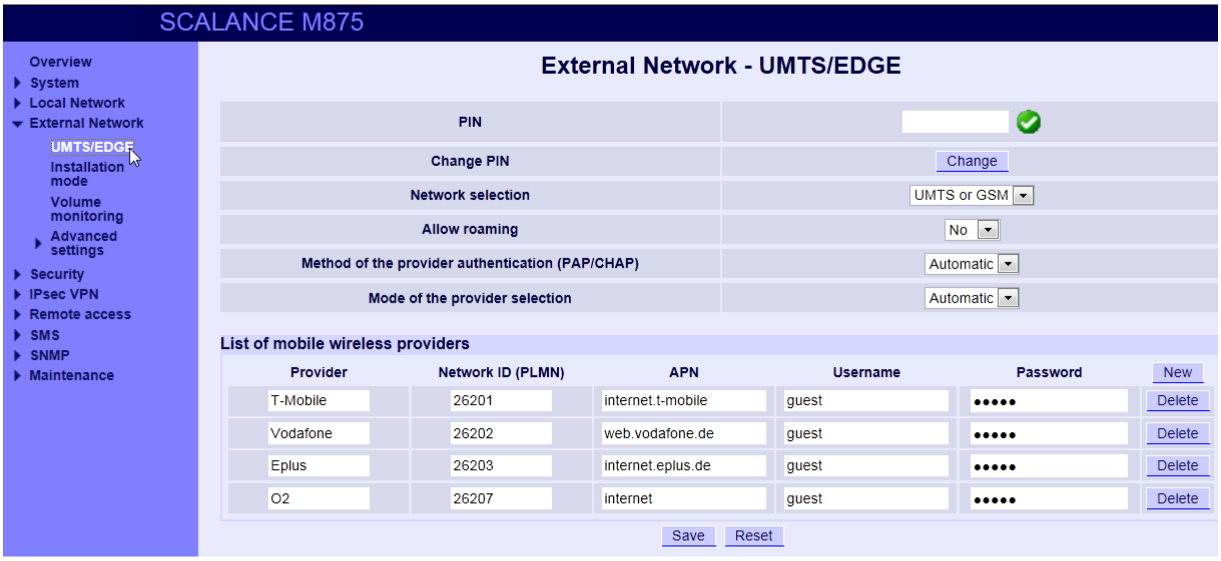
List of NTP servers for synchronization

NTP server	Polling interval
192.53.103.108	36,2h

Serve system time to local network: No

Enter the correct date and time and Local timezone. An NTP server can be selected to automatically synchronize the date and time. Keep in mind that using the NTP synchronization will use data from your data plan. Press the “Save” button when finished.

Step 13 – Overview of the External Network settings



External Network - UMTS/EDGE

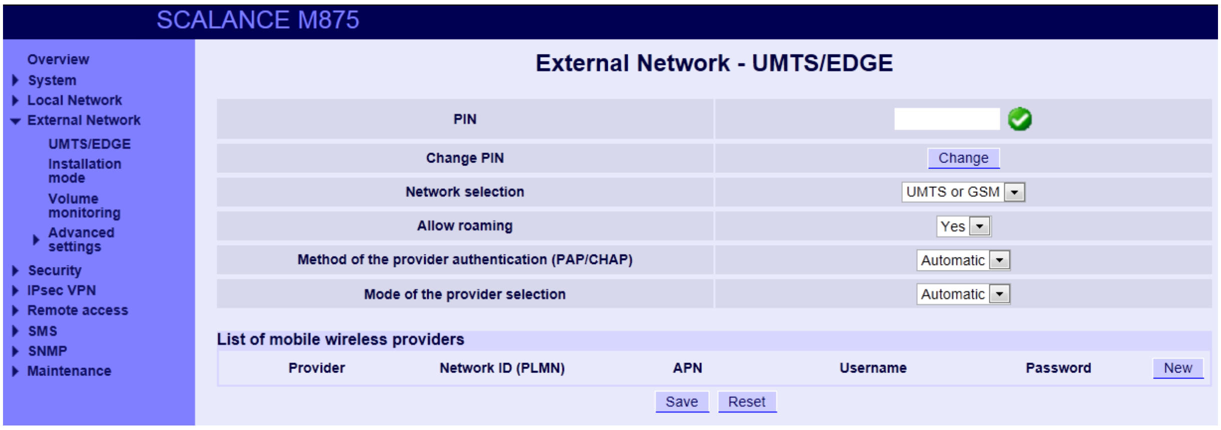
PIN	✓
Change PIN	Change
Network selection	UMTS or GSM
Allow roaming	No
Method of the provider authentication (PAP/CHAP)	Automatic
Mode of the provider selection	Automatic

List of mobile wireless providers

Provider	Network ID (PLMN)	APN	Username	Password	New
T-Mobile	26201	internet.t-mobile	guest	•••••	Delete
Vodafone	26202	web.vodafone.de	guest	•••••	Delete
Eplus	26203	internet.eplus.de	guest	•••••	Delete
O2	26207	internet	guest	•••••	Delete

Shown are the default “External Network – UMTS/EDGE” settings.

Step 14 – Configure the External Network settings



External Network - UMTS/EDGE

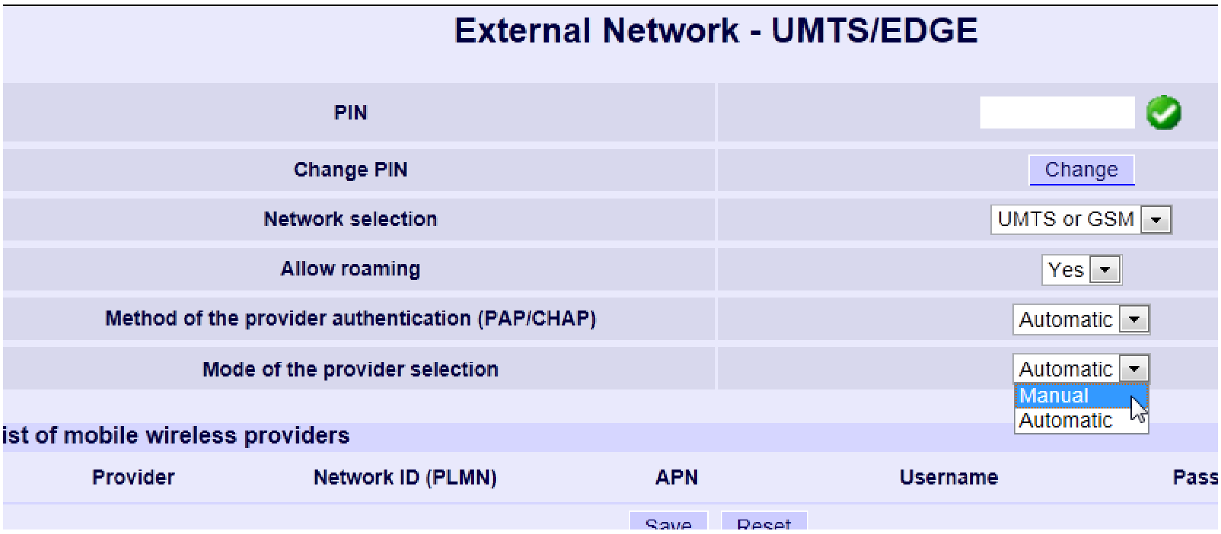
PIN	✓
Change PIN	Change
Network selection	UMTS or GSM
Allow roaming	Yes
Method of the provider authentication (PAP/CHAP)	Automatic
Mode of the provider selection	Automatic

List of mobile wireless providers

Provider	Network ID (PLMN)	APN	Username	Password	New

For our application enable “Allow roaming” and delete all the “List of moble wireless providers” and press “Save”. Make sure to check with your provider if you are charged extra for roaming. Only enable roaming if required for your application – 2G Partner connection.

Step 15 – Change Provider Mode to Manual



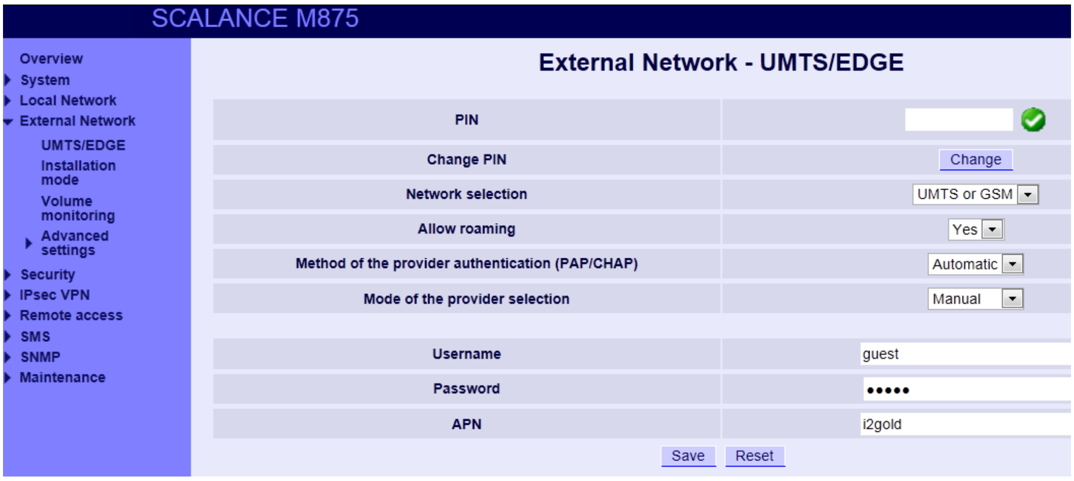
External Network - UMTS/EDGE

PIN	✓
Change PIN	Change
Network selection	UMTS or GSM
Allow roaming	Yes
Method of the provider authentication (PAP/CHAP)	Automatic
Mode of the provider selection	Automatic Manual Automatic

ist of mobile wireless providers

Provider	Network ID (PLMN)	APN	Username	Pass

Step 16 – Enter APN data for Manual mode



External Network - UMTS/EDGE

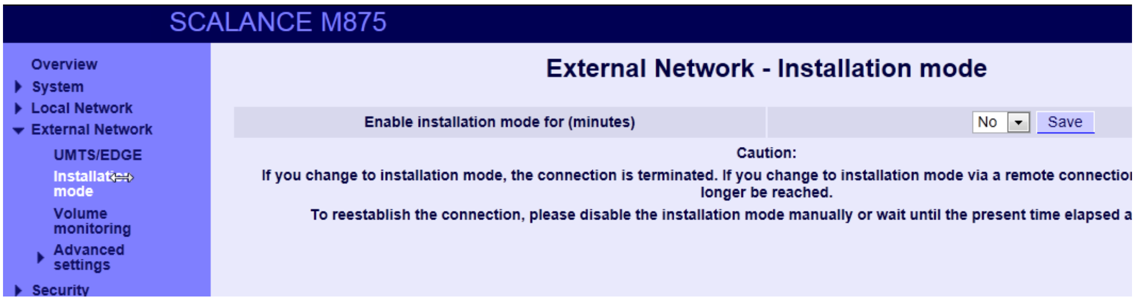
PIN	✓
Change PIN	Change
Network selection	UMTS or GSM
Allow roaming	Yes
Method of the provider authentication (PAP/CHAP)	Automatic
Mode of the provider selection	Manual
Username	guest
Password	•••••
APN	i2gold

Enter the correct APN data for your data plan and press “Save”. If using the Siemens Demo SIM enter:

- Username – guest
- Password – guest
- APN – i2gold or ccspbsc197.acfes.org – depends on the demo case

Note: If you are using a Partner 2G signal you will need to use “UMTS or GSM” and “Allow Roaming” for your system to function properly.

Step 17 – Enable Installation mode



External Network - Installation mode

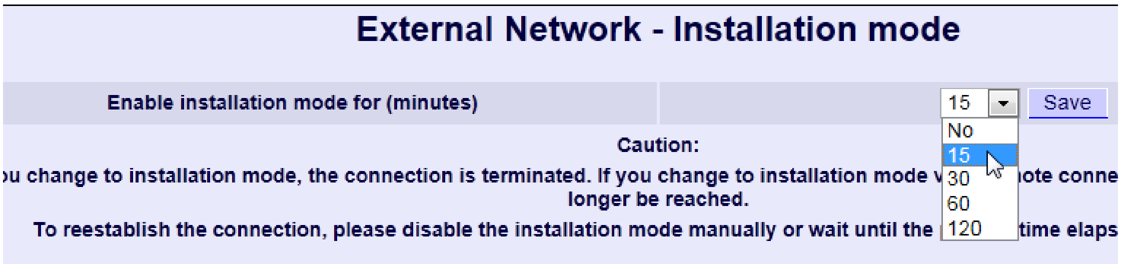
Enable installation mode for (minutes)

Caution:

If you change to installation mode, the connection is terminated. If you change to installation mode via a remote connectio longer be reached.

To reestablish the connection, please disable the installation mode manually or wait until the present time elapsed a

Installation mode is used for antennae alignment.



External Network - Installation mode

Enable installation mode for (minutes)

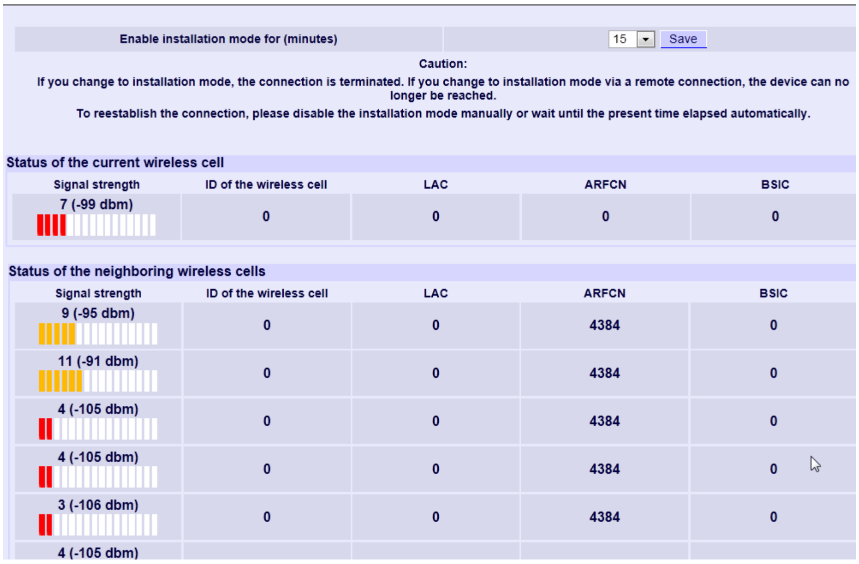
Caution:

›u change to installation mode, the connection is terminated. If you change to installation mode v ıote conne longer be reached.

To reestablish the connection, please disable the installation mode manually or wait until the time elaps

Select the time for Installation mode – 15 minutes should be adequate and press “Save”. Be sure to turn this back off when you are finished or you will not be able to finish connecting to your device.

Step 18 – Installation Mode enabled



Enable installation mode for (minutes)

Caution:

If you change to installation mode, the connection is terminated. If you change to installation mode via a remote connection, the device can no longer be reached.

To reestablish the connection, please disable the installation mode manually or wait until the present time elapsed automatically.

Status of the current wireless cell

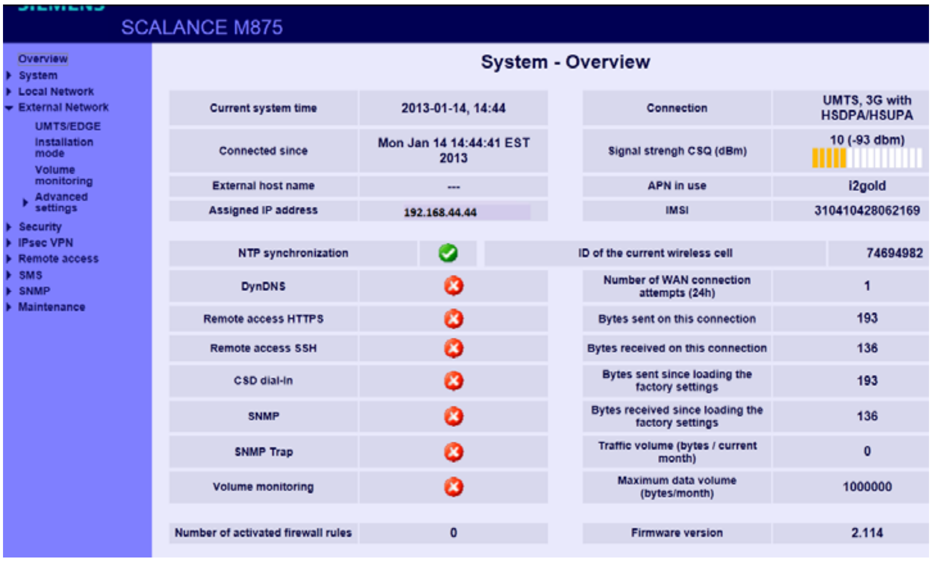
Signal strength	ID of the wireless cell	LAC	ARFCN	BSIC
7 (-99 dbm)	0	0	0	0

Status of the neighboring wireless cells

Signal strength	ID of the wireless cell	LAC	ARFCN	BSIC
9 (-95 dbm)	0	0	4384	0
11 (-91 dbm)	0	0	4384	0
4 (-105 dbm)	0	0	4384	0
4 (-105 dbm)	0	0	4384	0
3 (-106 dbm)	0	0	4384	0
4 (-105 dbm)				

Adjust antennae until the best signal is received. Either let the time out occur for Insatllation mode or change back to “No” and select “Save”.

Step 19 – Overview page after allignment



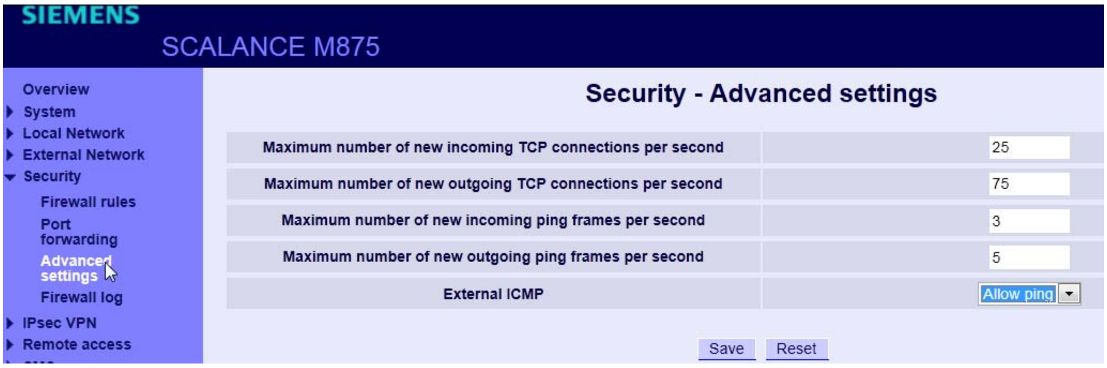
System - Overview

Current system time	2013-01-14, 14:44	Connection	UMTS, 3G with HSDPA/HSUPA
Connected since	Mon Jan 14 14:44:41 EST 2013	Signal strengh CSQ (dBm)	10 (-93 dbm)
External host name	---	APN in use	i2gold
Assigned IP address	192.168.44.44	IMSI	310410428062169
NTP synchronization	✓	ID of the current wireless cell	74694982
DynDNS	☒	Number of WAN connection attempts (24h)	1
Remote access HTTPS	☒	Bytes sent on this connection	193
Remote access SSH	☒	Bytes received on this connection	136
CSD dial-in	☒	Bytes sent since loading the factory settings	193
SNMP	☒	Bytes received since loading the factory settings	136
SNMP Trap	☒	Traffic volume (bytes / current month)	0
Volume monitoring	☒	Maximum data volume (bytes/month)	1000000
Number of activated firewall rules	0	Firmware version	2.114

After alignment, it may take a few minutes, but additional information should now be displayed in the Overview screen.

- Connected Since
- Assigned IP address – instead of 192.168.44.44 it would show the actual IP address of the SIM card or the dynamic IP address
- APN in use
- ID of the current wireless cell

Step 20 – Security settings for ping



Security - Advanced settings

Maximum number of new incoming TCP connections per second	25
Maximum number of new outgoing TCP connections per second	75
Maximum number of new incoming ping frames per second	3
Maximum number of new outgoing ping frames per second	5
External ICMP	Allow ping

To test the connection go to the “Security” “Advanced settings” and set the “External ICMP” to “Allow ping” and press “Save”. You should now be able to ping the IP address from the overview page from a computer connected to the internet.

Note

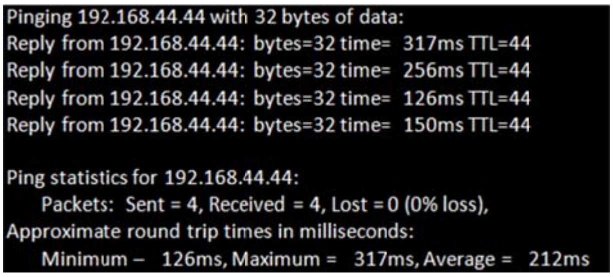
Increased costs due to extra data traffic

By sending the ping packets, the data traffic on the UMTS/GPRS connection is increased.

This may result in additional costs, depending on your user agreement with the mobile wireless provider.

Step 21 – Ping the M875 from the Internet

Disconnect your PC from the M875 or use a different computer that has a connection to the internet. Ping the IP address shown in the Overview page.

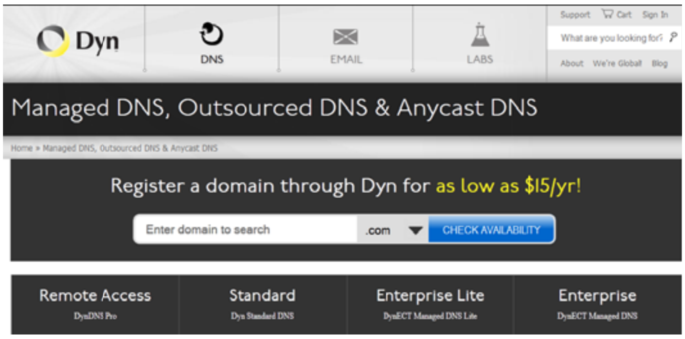


```
Pinging 192.168.44.44 with 32 bytes of data:
Reply from 192.168.44.44: bytes=32 time= 317ms TTL=44
Reply from 192.168.44.44: bytes=32 time= 256ms TTL=44
Reply from 192.168.44.44: bytes=32 time= 126ms TTL=44
Reply from 192.168.44.44: bytes=32 time= 150ms TTL=44

Ping statistics for 192.168.44.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum – 126ms, Maximum = 317ms, Average = 212ms
```

You can decide to leave Ping enabled on the M875 or for a more secure system "Discard" Ping. Make sure you plug the M875 back into your computer when finished. Keep in mind that leaving Ping enabled will use data from your data plan.

Step 22 – Dynamic IP address

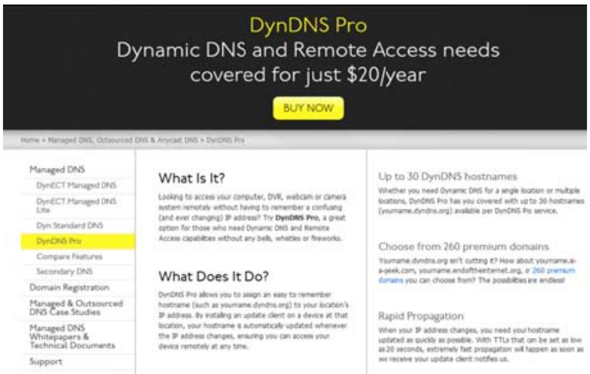
The Siemens Demo SIM has a fixed IP address, if you have a fixed IP address skip to step 25. If you get a Dynamic IP address from you provider you will need to also use a Dynamic DNS Server. You need to go to WWW.dyndns.org and create a profile.



Managed DNS, Outsourced DNS & Anycast DNS

Register a domain through Dyn for as low as $15/yr!

Select "Remote Access".


BUY NOW
Home » Managed DNS, Outsourced DNS & Anycast DNS » DynDNS Pro
Managed DNS
DynECT Managed DNS
DynECT Managed DNS Lite
Dyn Standard DNS
DynDNS Pro
Compare Features
Secondary DNS
Domain Registration
Managed & Outsourced DNS Case Studies
Managed DNS Whitepapers & Technical Documents
Support

DynDNS Pro
Dynamic DNS and Remote Access needs covered for just $20/year

What Is It?

Looking to access your computer, DVR, webcam or camera system remotely without having to remember a confusing (and ever changing) IP address? Try **DynDNS Pro**, a great option for those who need Dynamic DNS and Remote Access capabilities without any bells, whistles or fireworks.

What Does It Do?

DynDNS Pro allows you to assign an easy to remember hostname (such as yourname.dyndns.org) to your location's IP address. By installing an update client on a device at that location, your hostname is automatically updated whenever the IP address changes, ensuring you can access your device remotely at any time.

Up to 30 DynDNS hostnames

Whether you need Dynamic DNS for a single location or multiple locations, DynDNS Pro has you covered with up to 30 hostnames (yourname.dyndns.org) available per DynDNS Pro service.

Choose from 260 premium domains

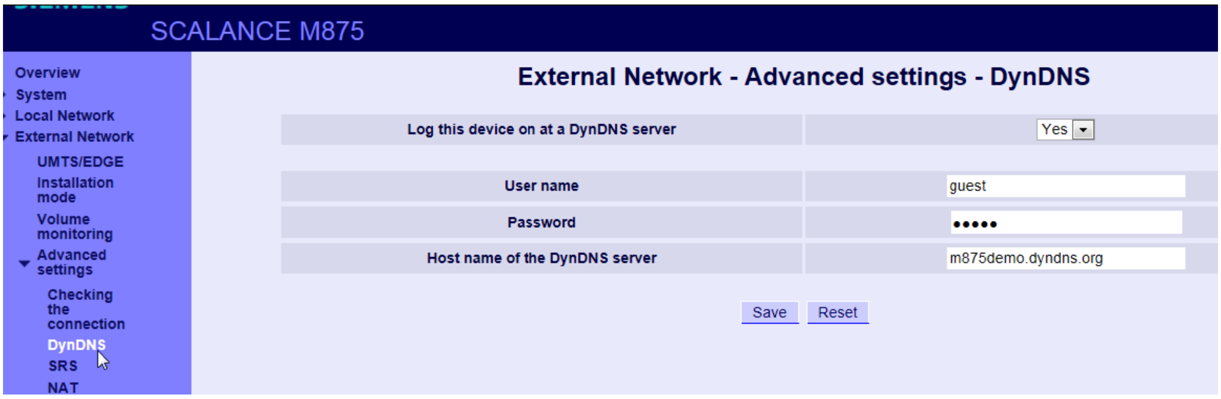
Yourname.dyndns.org isn't cutting it? How about yourname.is-a-geek.com, yourname.endoftheinternet.org, or 260 premium domains you can choose from? The possibilities are endless!

Rapid Propagation

When your IP address changes, you need your hostname updated as quickly as possible. With TTLs that can be set as low as 20 seconds, extremely fast propagation will happen as soon as we receive your update client notifies us.

Purchase the DynDNS Pro and register a DNS name for your M875 connection. The DNS name must use "dyndns.org" as the extension for example "brkm875.dyndns.org". The IP address used must also reflect the Dynamic IP address that was shown on the M875 "System Overview" screen – do not use the IP address shown in this demo.

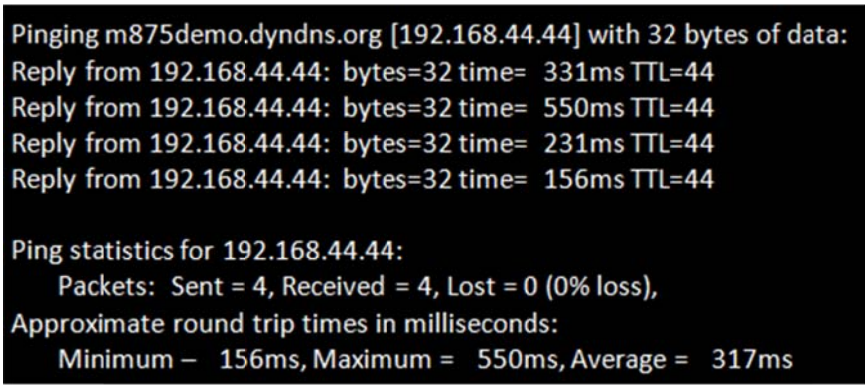
Step 23 – Enter the dyndns server host name



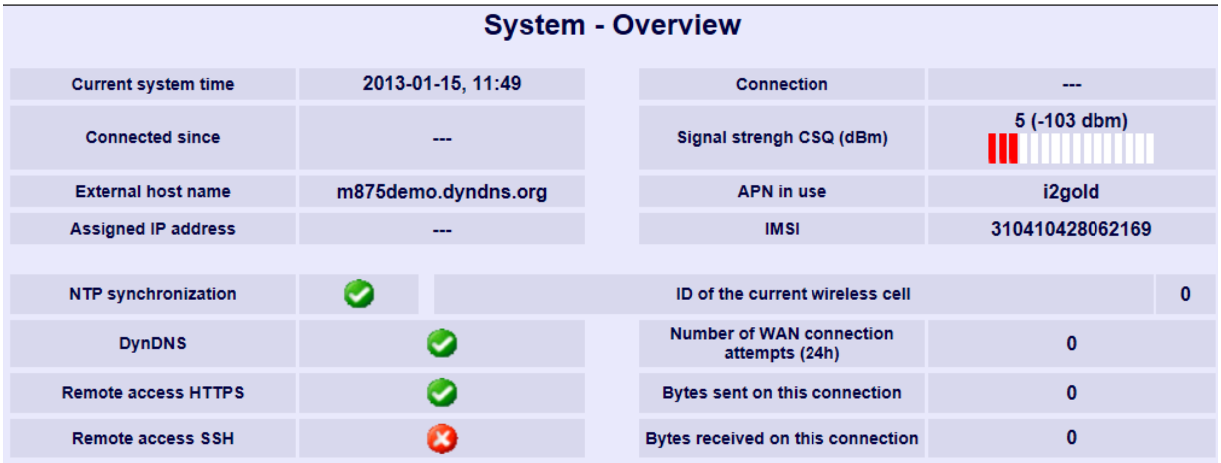
External Network - Advanced settings - DynDNS

Log this device on at a DynDNS server	Yes
User name	guest
Password	●●●●●
Host name of the DynDNS server	m875demo.dyndns.org

Enter your DynDNS server host name for a dynamic IP address example : m875demo.dyndns.org. Press “Save”. You can now ping your device using the Host name. Make sure you set Ping “Accept” if you had turned it off in step 21 or you will get no response to your ping request.



```
Pinging m875demo.dyndns.org [192.168.44.44] with 32 bytes of data:
Reply from 192.168.44.44:  bytes=32 time=  331ms TTL=44
Reply from 192.168.44.44:  bytes=32 time=  550ms TTL=44
Reply from 192.168.44.44:  bytes=32 time=  231ms TTL=44
Reply from 192.168.44.44:  bytes=32 time=  156ms TTL=44

Ping statistics for 192.168.44.44:
    Packets:  Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum –   156ms, Maximum =   550ms, Average =   317ms
```

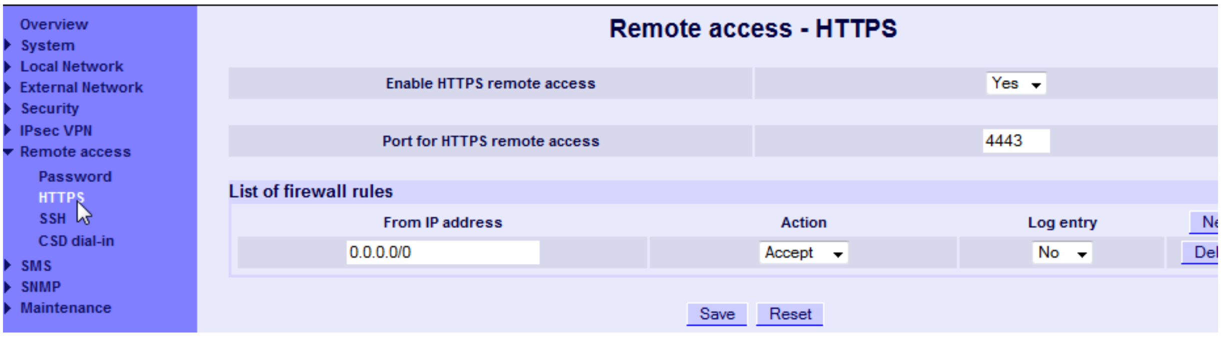


System - Overview

Current system time	2013-01-15, 11:49	Connection	---
Connected since	---	Signal strengh CSQ (dBm)	5 (-103 dbm)
External host name	m875demo.dyndns.org	APN in use	i2gold
Assigned IP address	---	IMSI	310410428062169
NTP synchronization	✓	ID of the current wireless cell	0
DynDNS	✓	Number of WAN connection attempts (24h)	0
Remote access HTTPS	✓	Bytes sent on this connection	0
Remote access SSH	✗	Bytes received on this connection	0

The System Overview screen will reflect the “External host name” as “m875demo.dyndns.org”. This may take a few minutes to show.

Step 24 – Configure Remote access



Remote access - HTTPS

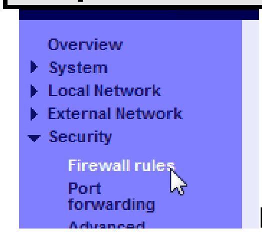
Enable HTTPS remote access	Yes
Port for HTTPS remote access	4443

List of firewall rules

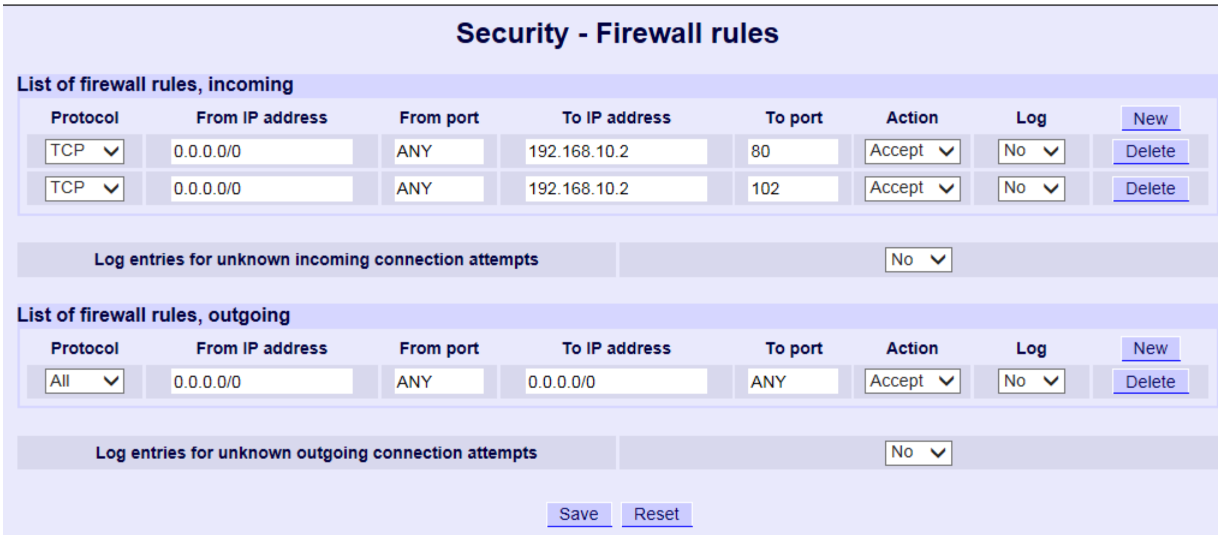
From IP address	Action	Log entry
0.0.0.0/0	Accept	No

Select “Yes” to enable HTTPS remote access, change the Port to 4443 in case you want to use Port 443 to allow restricted logon access to the PLC. You will also need to add a firewall rule to allow a connection “From IP address”. This IP address can be a specific address or if you leave it as “0.0.0.0/0” then anyone can try and access it. This is why a secure password is critical. I would suggest that you enter the IP address that is assigned to your location to keep others from gaining access or do not enable remote access. To test the connection the computer must have internet access, using Internet Explorer or Mozilla Firefox, enter for example https://192.168.44.44:4443 or https://m875demo.dyndns.org:4443 and you should get to the login screen.

Step 25 – Configure Firewall Rules



By default the Firewall is configured to block everything.



Security - Firewall rules

List of firewall rules, incoming

Protocol	From IP address	From port	To IP address	To port	Action	Log
TCP	0.0.0.0/0	ANY	192.168.10.2	80	Accept	No
TCP	0.0.0.0/0	ANY	192.168.10.2	102	Accept	No

Log entries for unknown incoming connection attempts	No

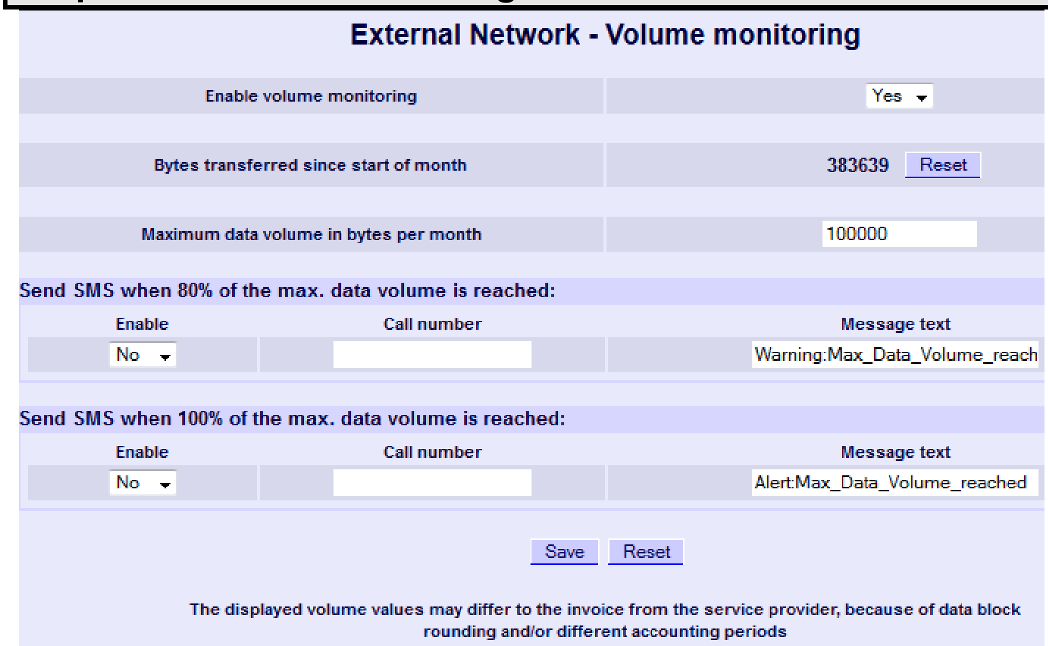
List of firewall rules, outgoing

Protocol	From IP address	From port	To IP address	To port	Action	Log
All	0.0.0.0/0	ANY	0.0.0.0/0	ANY	Accept	No

Log entries for unknown outgoing connection attempts	No

The firewall is configured to accept only TCP data incomming to our PLC (192.168.10.2) on Port 80 (Webserver) and Port 102 (Simatic Data).

Step 26 – Volume Monitoring



External Network - Volume monitoring

Enable volume monitoring	Yes
Bytes transferred since start of month	383639 Reset
Maximum data volume in bytes per month	100000

Send SMS when 80% of the max. data volume is reached:

Enable	Call number	Message text
No		Warning:Max_Data_Volume_reach

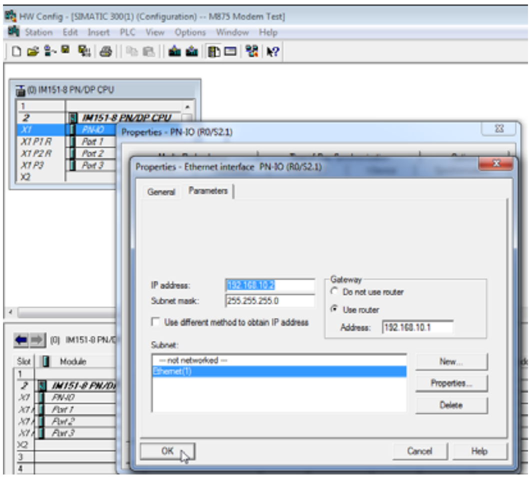
Send SMS when 100% of the max. data volume is reached:

Enable	Call number	Message text
No		Alert:Max_Data_Volume_reached

The displayed volume values may differ to the invoice from the service provider, because of data block rounding and/or different accounting periods

You can configure a text message to be sent warning of reaching a “maximum data usage per month”. This is only a message and will NOT stop the M875 from sending or receiving data. Your Data Plan Will Continue to Get Billed and you WILL be charged by the carrier for any data plan overage costs.

Step 27 – PLC Hardware Configuration



HW Config - [SIMATIC 300(1) (Configuration) -- M875 Modem Test]
Station Edit Insert PLC View Options Window Help
(0) IM151-8 PN/DP CPU
2 IM151-8 PN/DP CPU
X1 PN-IO
X1 P1 R Port 1
X1 P2 R Port 2
X1 P3 Port 3
X2
Properties - PN-IO (R0/S2.1)
Properties - Ethernet interface PN-IO (R0/S2.1)
General
Parameters
Slot
Module
New...
Properties...
Delete
OK
Cancel
Help

IP address: 192.168.10.2

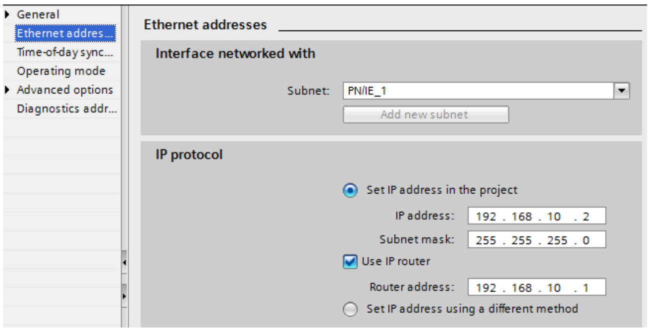
Subnet mask: 255.255.255.0

□ Use different method to obtain IP address

Gateway: ○ Do not use router ● Use router

Address: 192.168.10.1

Subnet: -- not networked -- / Ethernet(1)



Subnet: PN/IE_1

● Set IP address in the project

IP address: 192 . 168 . 10 . 2

Subnet mask: 255 . 255 . 255 . 0

☑ Use IP router

Router address: 192 . 168 . 10 . 1

○ Set IP address using a different method

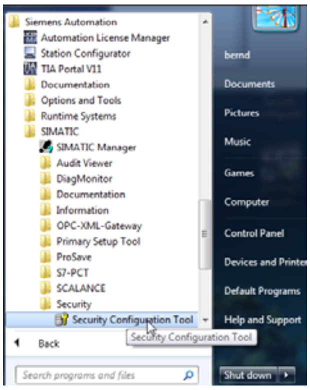
Step 7 V5.5

TIA Portal V11

Make sure the PLC configuration sets the IP address to an IP address in the range of 192.168.10.x and use router 192.168.10.1, then “Save and Comple”. Unplug your pc from the M875, plug the PC into the PLC and download the hardware configuration. Then disconnect the PC from the network and plug the PLC into the top Ethernet Port of the M875.

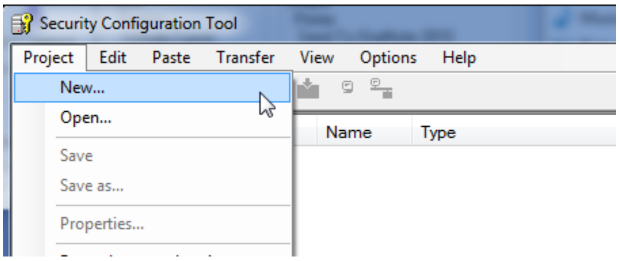
SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 28 – Create IPsec VPN Certificates - Security Configuration Tool



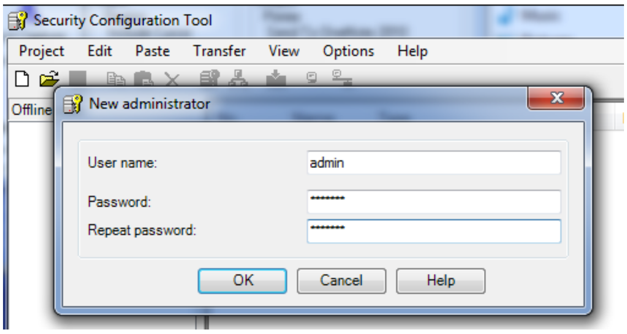
From the Windows "Start Menu" start the "Security Configuration Tool"

Step 29 – Start new project



Select "Project" "New"

Step 30 – Create project User name and password



User name: admin

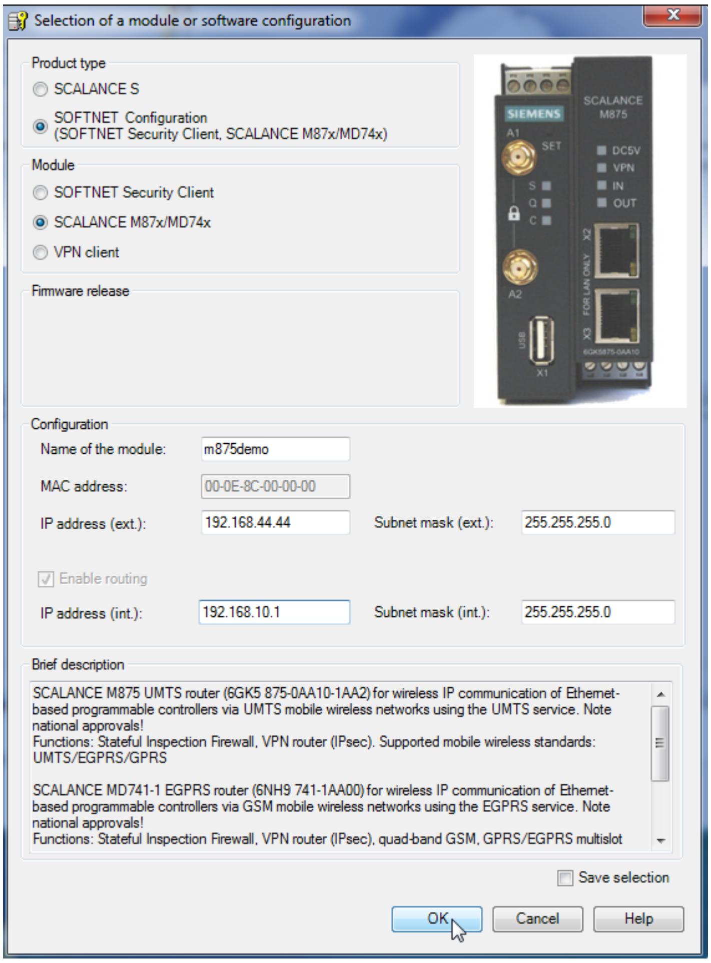
Password: ********

Repeat password: ********

Enter a User name and password for the project.

For this demo User name: admin and Password: siemens1 – all lower case. For a real project you should not use "admin" as the user and make a secure password using upper case, lower case, numbers, and special characters – see step 8 for example. The password must be at least 8 characters.

Step 31 – Configure the M875 IP address



Selection of a module or software configuration

Product type

○ SCALANCE S

● SOFTNET Configuration (SOFTNET Security Client, SCALANCE M87x/MD74x)

Module

○ SOFTNET Security Client

● SCALANCE M87x/MD74x

○ VPN client

Firmware release

Configuration

Name of the module: m875demo

MAC address: 00-0E-8C-00-00-00

IP address (ext.): 192.168.44.44 Subnet mask (ext.): 255.255.255.0

☑ Enable routing

IP address (int.): 192.168.10.1 Subnet mask (int.): 255.255.255.0

Brief description

SCALANCE M875 UMTS router (6GK5 875-0AA10-1AA2) for wireless IP communication of Ethernet-based programmable controllers via UMTS mobile wireless networks using the UMTS service. Note national approvals!
Functions: Stateful Inspection Firewall, VPN router (IPsec). Supported mobile wireless standards: UMTS/EGPRS/GPRS

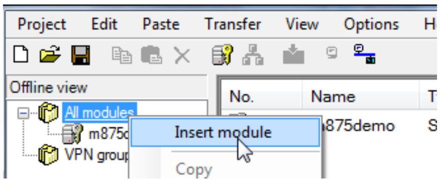
SCALANCE MD741-1 EGPRS router (6NH9 741-1AA00) for wireless IP communication of Ethernet-based programmable controllers via GSM mobile wireless networks using the EGPRS service. Note national approvals!
Functions: Stateful Inspection Firewall, VPN router (IPsec), quad-band GSM, GPRS/EGPRS multislot

□ Save selection

Enter the following:

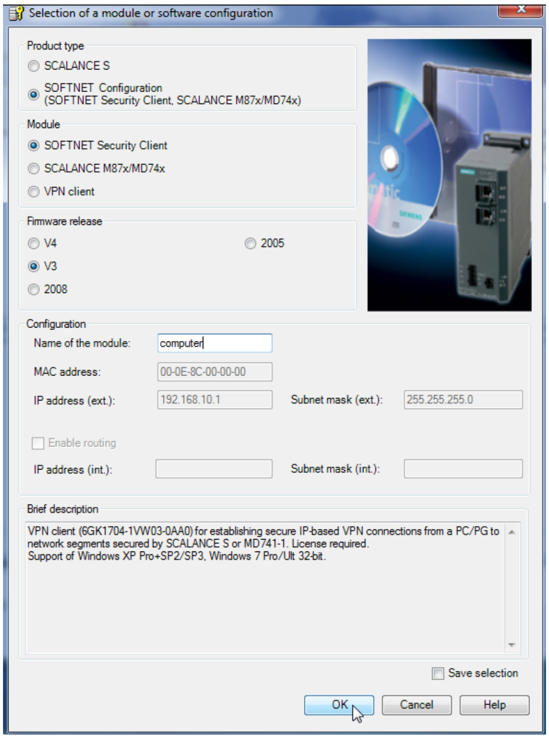
- Product type – SOFTNET Configuration
- Module – SCALANCE M87x/MD74x
- Name of the module – m875demo
- IP address (ext) – your AT&T SIM card IP address. If a Dynamic address was assigned just enter any address or use the address from the overview screen in step 19 which is the dynamic address that is temporarily assigned. For our demo 192.168.44.44 subnet 255.255.255.0– not a real address.
- IPaddress (int) - 192.168.10.1 subnet 255.255.255.0 – this is the nework that the PLC will be connected.
- Press "OK"

Step 32 – Insert Module



Insert next Module.

Step 33 – Configure Softnet Security Client Module



Product type
○ SCALANCE S
● SOFTNET Configuration (SOFTNET Security Client, SCALANCE M87x/MD74x)

Module
● SOFTNET Security Client
○ SCALANCE M87x/MD74x
○ VPN client

Firmware release
○ V4
○ 2005
● V3
○ 2008

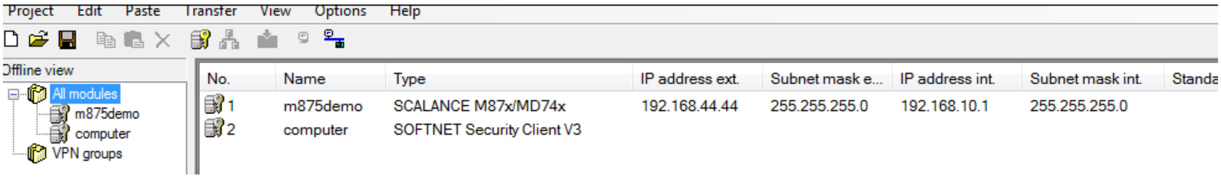
Configuration
Name of the module: computer
MAC address: 00-0E-8C-00-00-00
IP address (ext.): 192.168.10.1
Subnet mask (ext.): 255.255.255.0
□ Enable routing
IP address (int.):
Subnet mask (int.):

Brief description
VPN client (6GK1704-1VW03-0AA0) for establishing secure IP-based VPN connections from a PC/PG to network segments secured by SCALANCE S or MD741-1. License required.
Support of Windows XP Pro+SP2/SP3, Windows 7 Pro/Ult 32-bit.

□ Save selection

Enter the following:

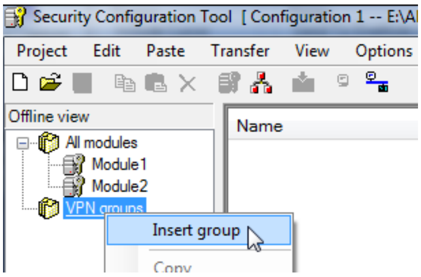
- Product type – SOFTNET Configuration
- Module – SOFTNET Security Client
- Firmware release – V3
- Name of the module - computer
- Press “OK”



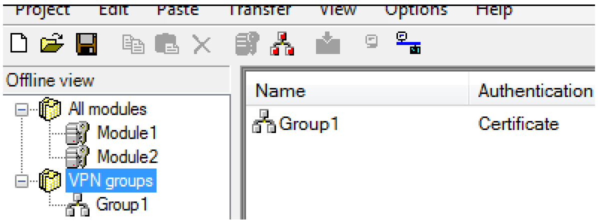
No.	Name	Type	IP address ext.	Subnet mask e...	IP address int.	Subnet mask int.	Standa
1	m875demo	SCALANCE M87x/MD74x	192.168.44.44	255.255.255.0	192.168.10.1	255.255.255.0	
2	computer	SOFTNET Security Client V3					

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 34 – Insert VPN Group

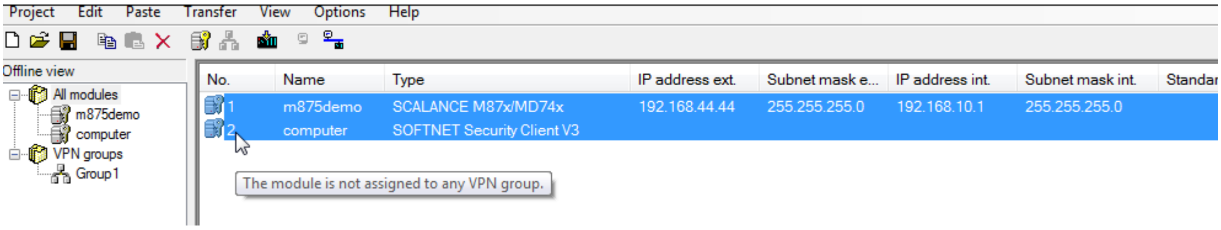


Insert a new “VPN group”



Name	Authentication
Group1	Certificate

Step 35 – Move into VPN Group

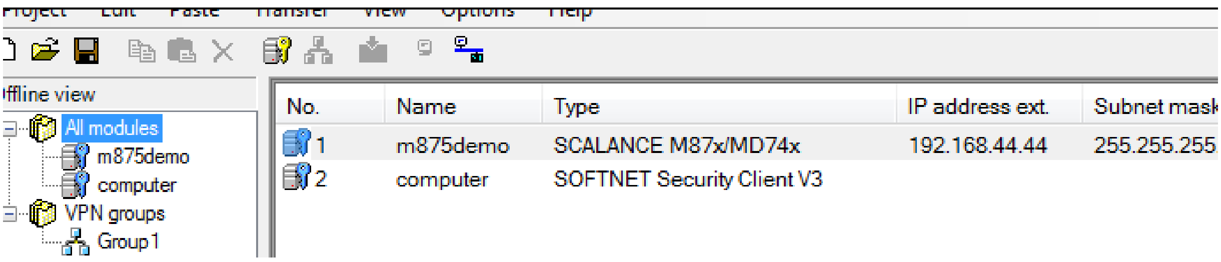


No.	Name	Type	IP address ext.	Subnet mask e...	IP address int.	Subnet mask int.	Standar
1	m875demo	SCALANCE M87x/MD74x	192.168.44.44	255.255.255.0	192.168.10.1	255.255.255.0	
2	computer	SOFTNET Security Client V3					

The module is not assigned to any VPN group.

Highlight “m875demo” and “computer” then drag and drop into the VPN “Group 1”

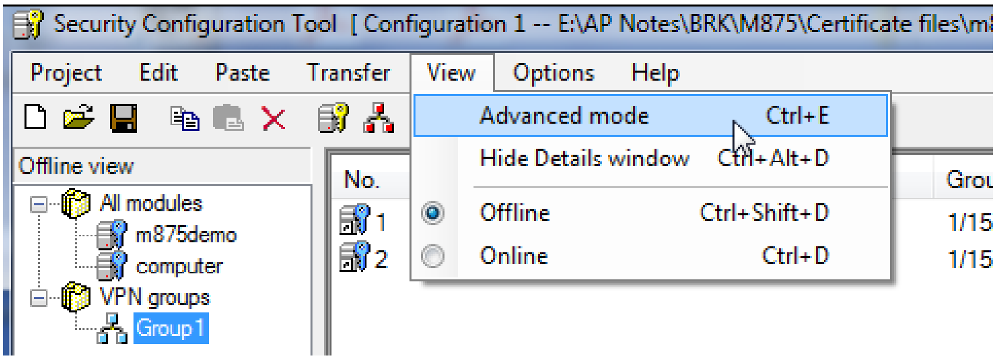
Step 36 – Certificate changes to blue



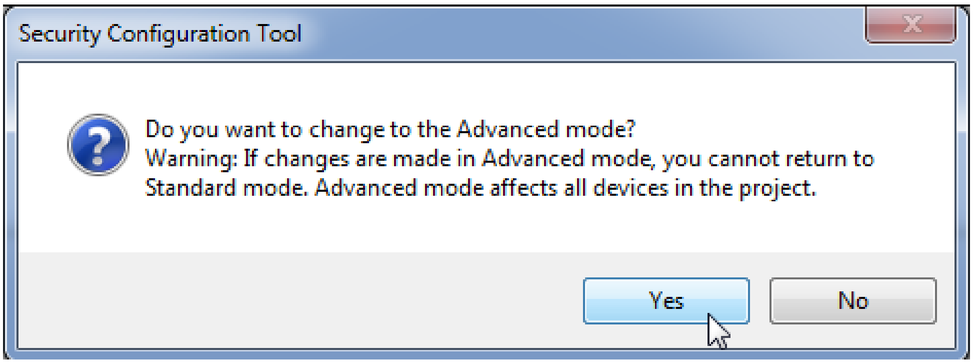
No.	Name	Type	IP address ext.	Subnet mask
1	m875demo	SCALANCE M87x/MD74x	192.168.44.44	255.255.255
2	computer	SOFTNET Security Client V3		

After the modules are put into the VPN “Group1” the keys turn blue to show the VPN tunnel.

Step 37 – Advanced View


Security Configuration Tool [Configuration 1 -- E:\AP Notes\BRK\M875\Certificate files\m
Project Edit Paste Transfer View Options Help
Advanced mode Ctrl+E
Hide Details window Ctrl+Alt+D
Offline Ctrl+Shift+D
Online Ctrl+D
Offline view
All modules
m875demo
computer
VPN groups
Group1
No.
1
2
Grou
1/15
1/15

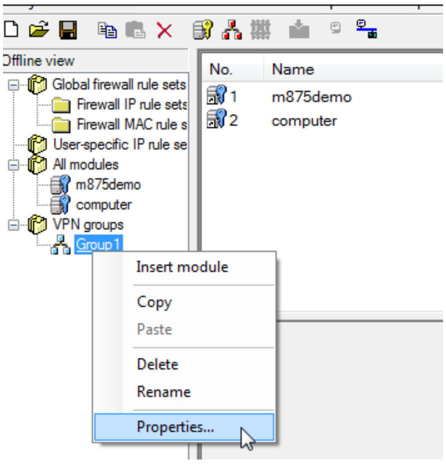
Change to “View” “Advanced mode”



Do you want to change to the Advanced mode?
Warning: If changes are made in Advanced mode, you cannot return to Standard mode. Advanced mode affects all devices in the project.

Select “Yes”

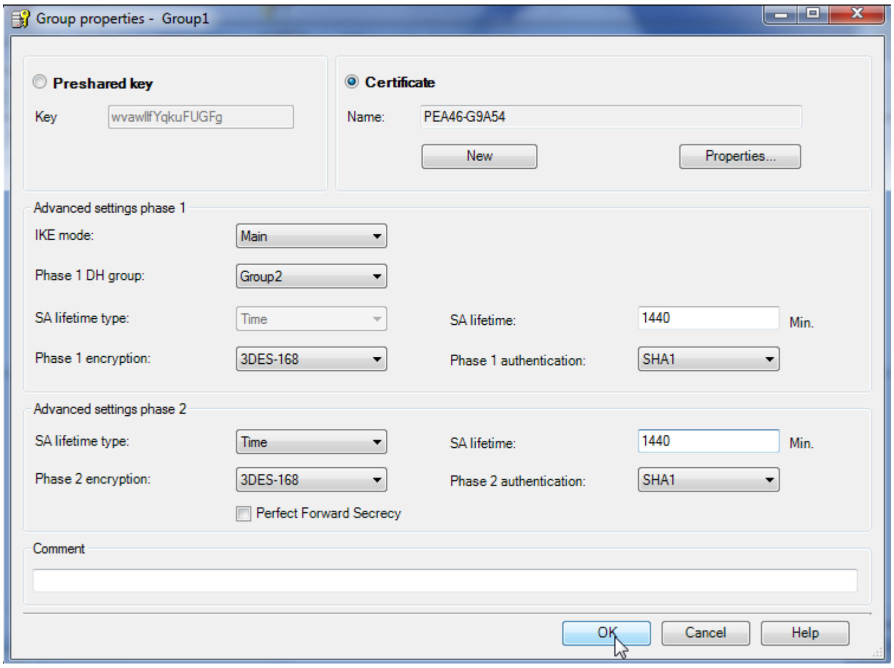
Step 38 – IPsec VPN Properties



Right mouse click on “Group1” and select “Properties”

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 39 – Modifiy IPsec VPN Properties



Group properties - Group1

○ Preshared key
Key: wvawlfYqkuFUGFg

● Certificate
Name: PEA46-G9A54

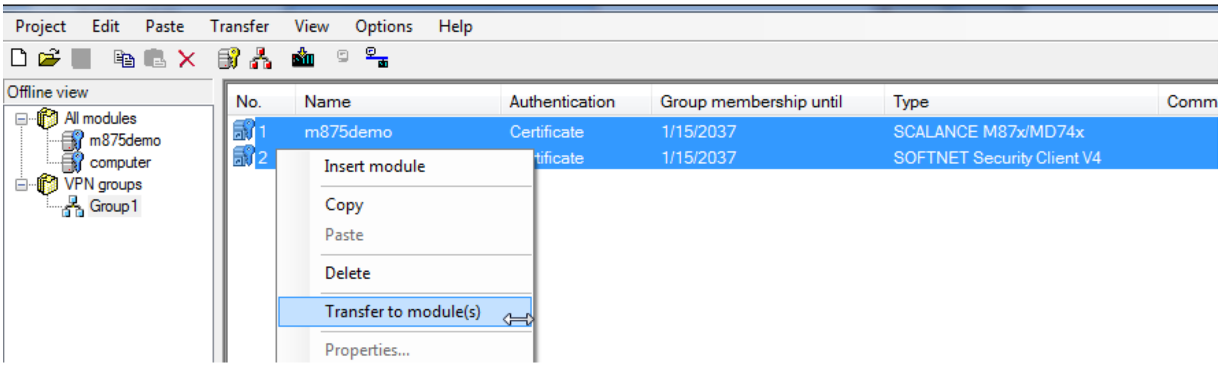
Advanced settings phase 1
IKE mode: Main
Phase 1 DH group: Group2
SA lifetime type: Time
SA lifetime: 1440 Min.
Phase 1 encryption: 3DES-168
Phase 1 authentication: SHA1

Advanced settings phase 2
SA lifetime type: Time
SA lifetime: 1440 Min.
Phase 2 encryption: 3DES-168
Phase 2 authentication: SHA1
□ Perfect Forward Secrecy

Comment

Make sure “SA lifetime” for both “phase 1” and “phase 2” is set to 1440 or the connection will not work. Press “OK” and then save the project.

Step 40 – Transfer Certificates to files

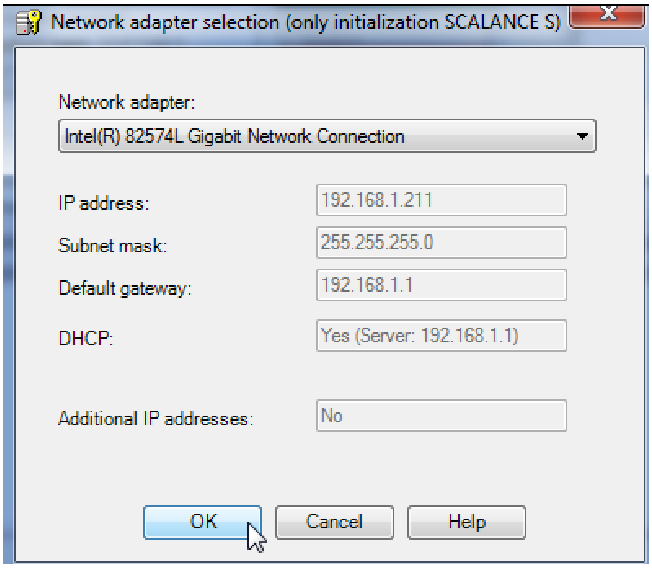


No.	Name	Authentication	Group membership until	Type	Comm
1	m875demo	Certificate	1/15/2037	SCALANCE M87x/MD74x	
2		tificate	1/15/2037	SOFTNET Security Client V4	

Highlight both the “m875demo” and “computer” certificates and then right mouse click and “Transfer to module(s)”. You do not need to be online with the M875, this is used only to create the certificate files.

SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 41 – Select Ethernet Adapter



Network adapter selection (only initialization SCALANCE S)

Network adapter: Intel(R) 82574L Gigabit Network Connection

IP address: 192.168.1.211

Subnet mask: 255.255.255.0

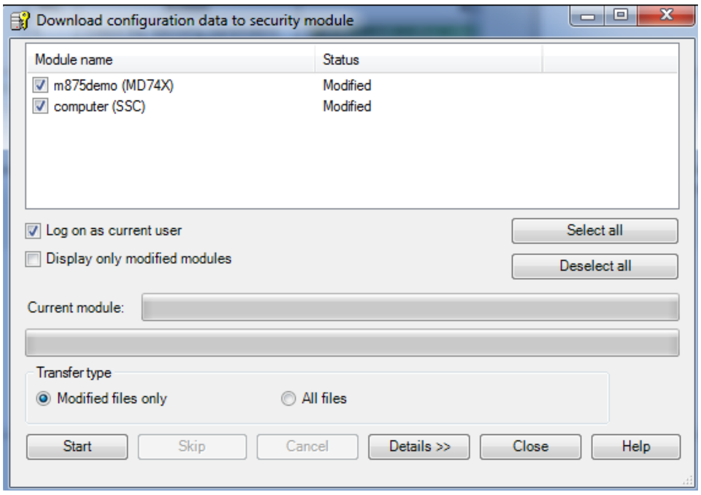
Default gateway: 192.168.1.1

DHCP: Yes (Server: 192.168.1.1)

Additional IP addresses: No

Select the Ethernet adapter that you will use to download SCT configurations. This can always be changed later. This screen may not appear if you have already used the software.

Step 42 – Start Certificate Transfer



Download configuration data to security module

Module name	Status
☑ m875demo (MD74X)	Modified
☑ computer (SSC)	Modified

☑ Log on as current user

□ Display only modified modules

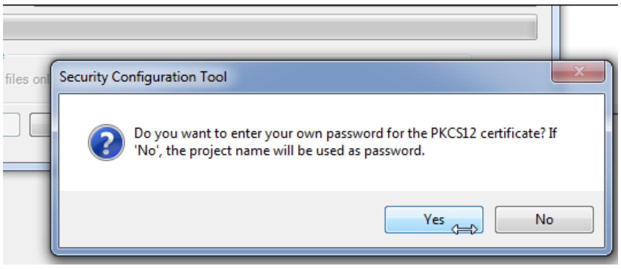
Current module:

Transfer type

● Modified files only ○ All files

Press “Start” to create the certificate files – you will be asked where to store the files.

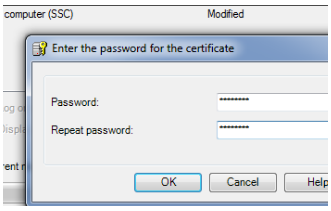
Step 43 – Set password



Security Configuration Tool

Do you want to enter your own password for the PKCS12 certificate? If 'No', the project name will be used as password.

Answer “Yes”

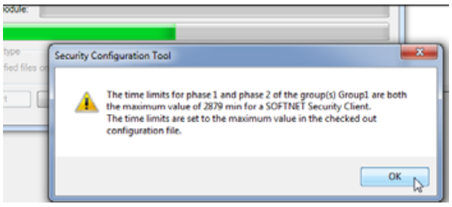


Enter the password for the certificate

Password: ********

Repeat password: ********

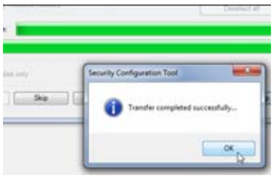
For the demo – “siemens1” is used.



Security Configuration Tool

The time limits for phase 1 and phase 2 of the group(s) Group1 are both the maximum value of 2879 min for a SOFTNET Security Client.
The time limits are set to the maximum value in the checked out configuration file.

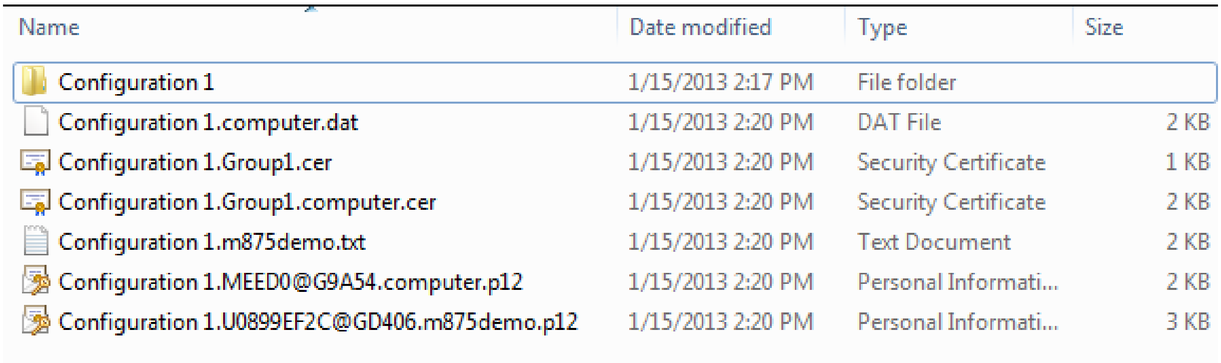
Select “OK”



Security Configuration Tool

Transfer completed successfully...

Step 44 – Certificate configuration Files created



Name	Date modified	Type	Size
Configuration 1	1/15/2013 2:17 PM	File folder	
Configuration 1.computer.dat	1/15/2013 2:20 PM	DAT File	2 KB
Configuration 1.Group1.cer	1/15/2013 2:20 PM	Security Certificate	1 KB
Configuration 1.Group1.computer.cer	1/15/2013 2:20 PM	Security Certificate	2 KB
Configuration 1.m875demo.txt	1/15/2013 2:20 PM	Text Document	2 KB
Configuration 1.MEED0@G9A54.computer.p12	1/15/2013 2:20 PM	Personal Informati...	2 KB
Configuration 1.U0899EF2C@GD406.m875demo.p12	1/15/2013 2:20 PM	Personal Informati...	3 KB

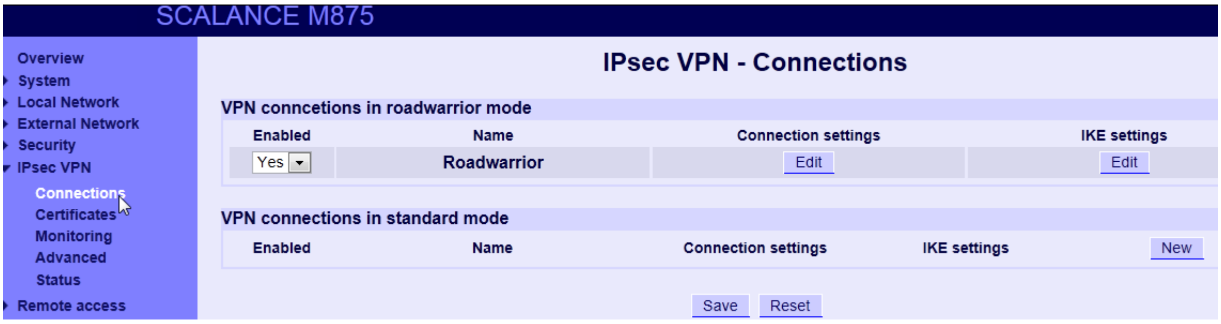
The above Certificate files should have been created.

Step 45 – IPsec VPN configuration text file

Open the text file that was created when the certificate was made for example “Configuration1.m875demo.txt”. It will contain the following information:

```
IPSec VPN > Certificates
   Upload Remote Site Certificate: Configuration 1.Group1.computer.cer
   Upload PKCS12 File (.p12): Configuration 1.U0899EF2C@GD406.m875demo.p12

IPSec VPN > Connections > VPN Roadwarrior Mode - Edit Settings
   Authentication method: X.509 Remote Certificate
   Remote Certificate: Configuration 1.Group1.computer.cer
   Remote ID: U1BEF40D2@GD406

IPSec VPN > Connections > VPN Roadwarrior Mode - Edit IKE
   Phase 1 - ISAKMP SA
   ISAKMP-SA encryption: 3DES-168
   ISKAMP-SA hash: SHA-1
   ISKAMP-SA mode: Main Mode
   ISAKMP-SA lifetime (seconds): 86400

   Phase 2 - IPSec SA
   IPSec-SA encryption: 3DES-168
   IPSec-SA hash: SHA-1
   IPSec-SA lifetime (seconds): 86400

   NAT-T: On
   Activate Dead Peer Detection: Yes
   DPD-Delay (seconds): 150
   DPD-timeout (seconds): 60
   DPD-maximum failure: 5
```

Step 46 – IPsec VPN Configuration - Roadwarrior



IPsec VPN - Connections

VPN conncetions in roadwarrior mode

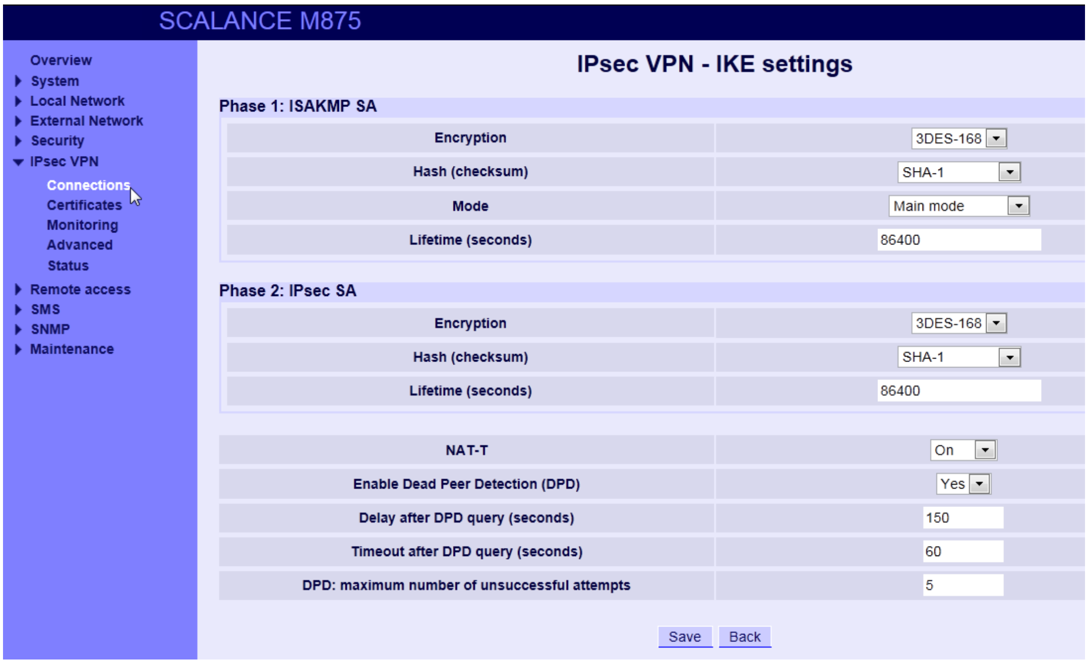
Enabled	Name	Connection settings	IKE settings
Yes	Roadwarrior	Edit	Edit

VPN connections in standard mode

Enabled	Name	Connection settings	IKE settings

Enable “Roadwarrior” mode and select “Save”. Select “IKE settings” “Edit”.

Step 47 – IKE Settings



IPsec VPN - IKE settings

Phase 1: ISAKMP SA

Encryption	3DES-168
Hash (checksum)	SHA-1
Mode	Main mode
Lifetime (seconds)	86400

Phase 2: IPsec SA

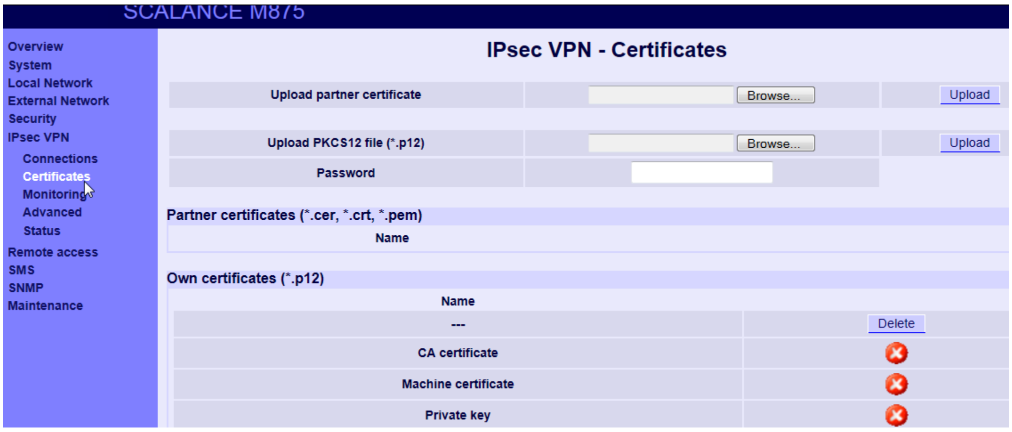
Encryption	3DES-168
Hash (checksum)	SHA-1
Lifetime (seconds)	86400

NAT-T	On
Enable Dead Peer Detection (DPD)	Yes
Delay after DPD query (seconds)	150
Timeout after DPD query (seconds)	60
DPD: maximum number of unsuccessful attempts	5

From step 26 we get the following information to enter. Then press “Save”:

- Encryption – 3DES-168
- Hash (checksum) – SHA-1
- Mode – Main mode
- Lifetime(seconds) – 86400
- NAT-T – On
- Enable Dead Peer Detection (DPD) – Yes
- Delay after DPD query (seconds) – 150
- Timout after DPD query (seconds) – 60
- DPD: maximum number of unsuccessful attempts - 5

Step 48 – IPsec VPN – Certificates



SCALANCE M875

- Overview
- System
- Local Network
- External Network
- Security
- IPsec VPN
  - Connections
  - Certificates
  - Monitoring
  - Advanced
  - Status
- Remote access
- SMS
- SNMP
- Maintenance

IPsec VPN - Certificates

Upload partner certificate	Browse...	Upload
Upload PKCS12 file (*.p12)	Browse...	Upload
Password		

Partner certificates (*.cer, *.crt, *.pem)

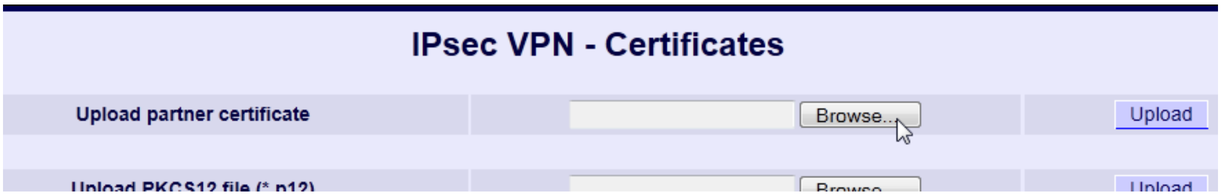
Name

Own certificates (*.p12)

Name	
---	Delete
CA certificate	✗
Machine certificate	✗
Private key	✗

The certificates page shows status information and certificates can be uploaded to the M875

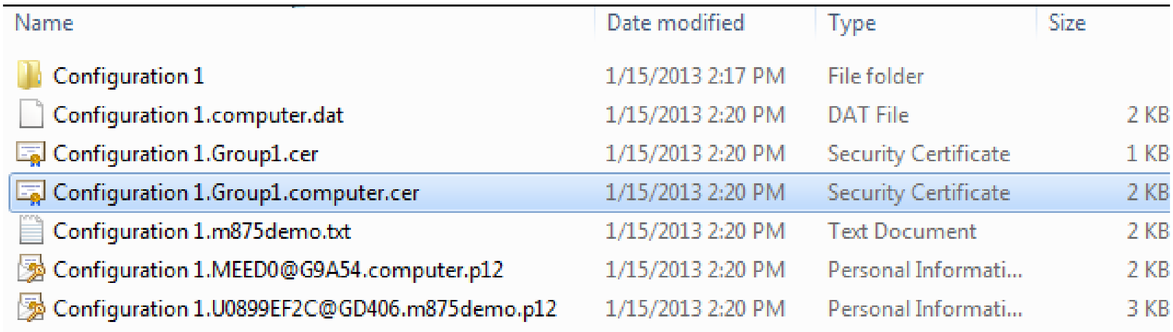
Step 56 – IPsec VPN – upoad partner certificate



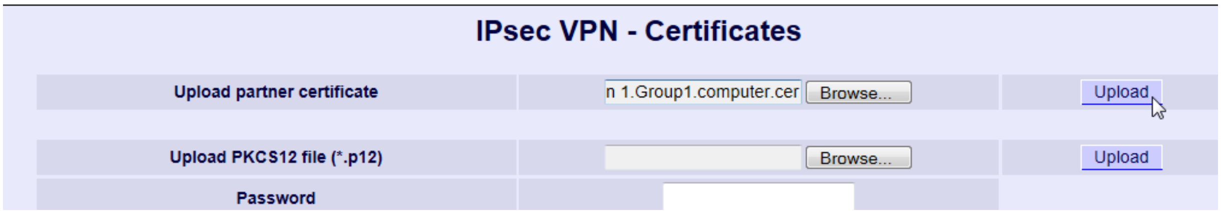
IPsec VPN - Certificates

Upload partner certificate	Browse...	Upload
Upload PKCS12 file (*.p12)	Browse...	Upload

Browse to the directory where you saved the certificates. From step 43 we see that the file needed is Remote Site Certificate: Configuration 1.Group1.computer.cer



Name	Date modified	Type	Size
Configuration 1	1/15/2013 2:17 PM	File folder	
Configuration 1.computer.dat	1/15/2013 2:20 PM	DAT File	2 KB
Configuration 1.Group1.cer	1/15/2013 2:20 PM	Security Certificate	1 KB
Configuration 1.Group1.computer.cer	1/15/2013 2:20 PM	Security Certificate	2 KB
Configuration 1.m875demo.txt	1/15/2013 2:20 PM	Text Document	2 KB
Configuration 1.MEED0@G9A54.computer.p12	1/15/2013 2:20 PM	Personal Informati...	2 KB
Configuration 1.U0899EF2C@GD406.m875demo.p12	1/15/2013 2:20 PM	Personal Informati...	3 KB



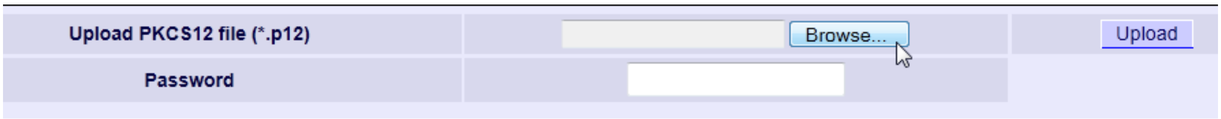
IPsec VPN - Certificates

Upload partner certificate	n 1.Group1.computer.cer Browse...	Upload
Upload PKCS12 file (*.p12)	Browse...	Upload
Password		

Select the partner certificate you created and then “Upload”. It uploads almost instantly, the certificate pah in “Browse” will no longer appear when complete.

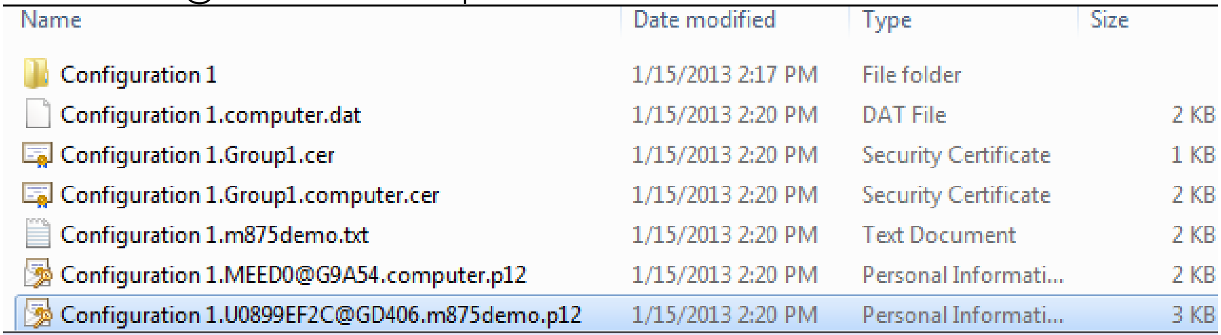
SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 49 – Upload PKCS12 file

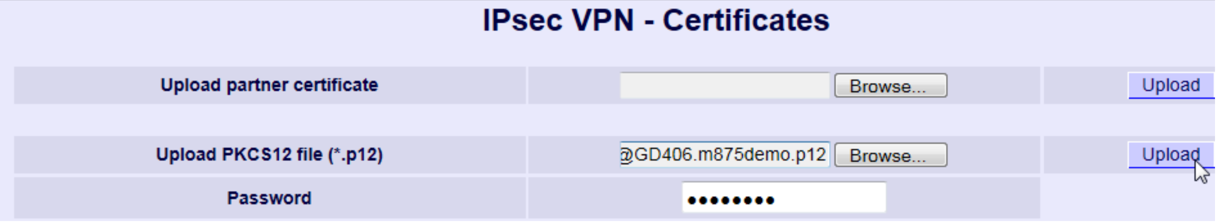


Upload PKCS12 file (*.p12)	Browse...	Upload
Password		

Browse to the directory where you saved the certificates and select the file for the M875. From step 43 we see that the file needed is PKCS12 File (.p12): Configuration 1.U0899EF2C@GD406.m875demo.p12



Name	Date modified	Type	Size
Configuration 1	1/15/2013 2:17 PM	File folder	
Configuration 1.computer.dat	1/15/2013 2:20 PM	DAT File	2 KB
Configuration 1.Group1.cer	1/15/2013 2:20 PM	Security Certificate	1 KB
Configuration 1.Group1.computer.cer	1/15/2013 2:20 PM	Security Certificate	2 KB
Configuration 1.m875demo.txt	1/15/2013 2:20 PM	Text Document	2 KB
Configuration 1.MEED0@G9A54.computer.p12	1/15/2013 2:20 PM	Personal Informati...	2 KB
Configuration 1.U0899EF2C@GD406.m875demo.p12	1/15/2013 2:20 PM	Personal Informati...	3 KB

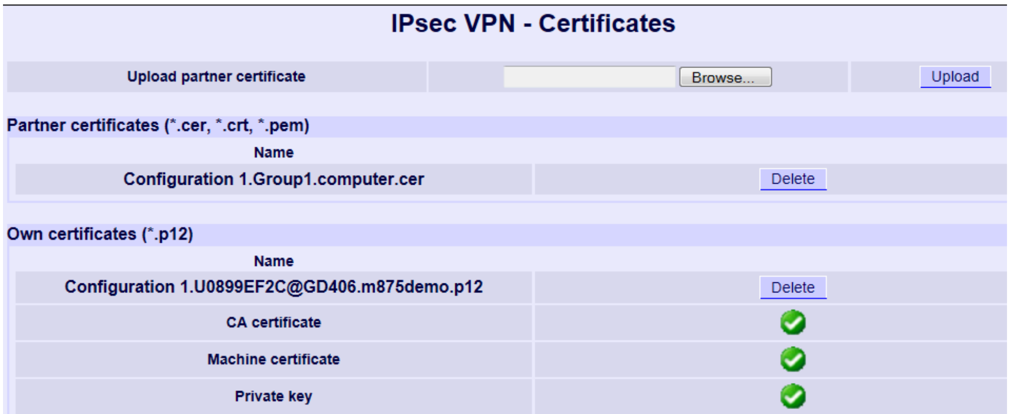


IPsec VPN - Certificates

Upload partner certificate	Browse...	Upload
Upload PKCS12 file (*.p12)	@GD406.m875demo.p12 Browse...	Upload
Password	••••••••	

Enter the password that was created with the certificate and press “Upload”. The upload happens very quickly.

Step 50 – Certificate validation



IPsec VPN - Certificates

Upload partner certificate	Browse...	Upload

Partner certificates (*.cer, *.crt, *.pem)

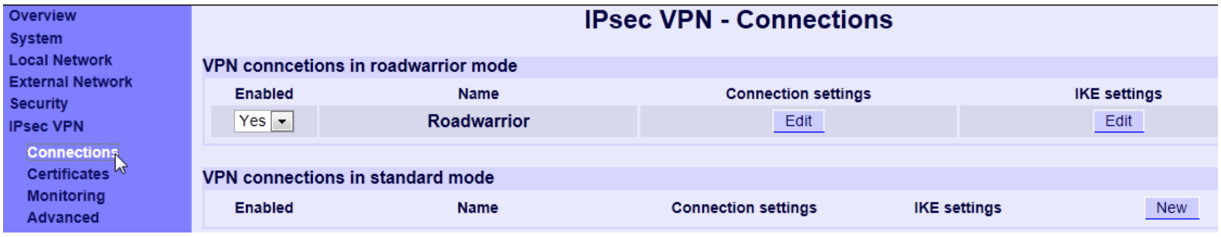
Name	
Configuration 1.Group1.computer.cer	Delete

Own certificates (*.p12)

Name	
Configuration 1.U0899EF2C@GD406.m875demo.p12	Delete
CA certificate	✓
Machine certificate	✓
Private key	✓

If everything matches there will be green check marks as shown. If not you will need to verify that the certificates were created correctly and that the correct password and files were uploaded.

Step 51 – IPsec VPN Conections settings



IPsec VPN - Connections

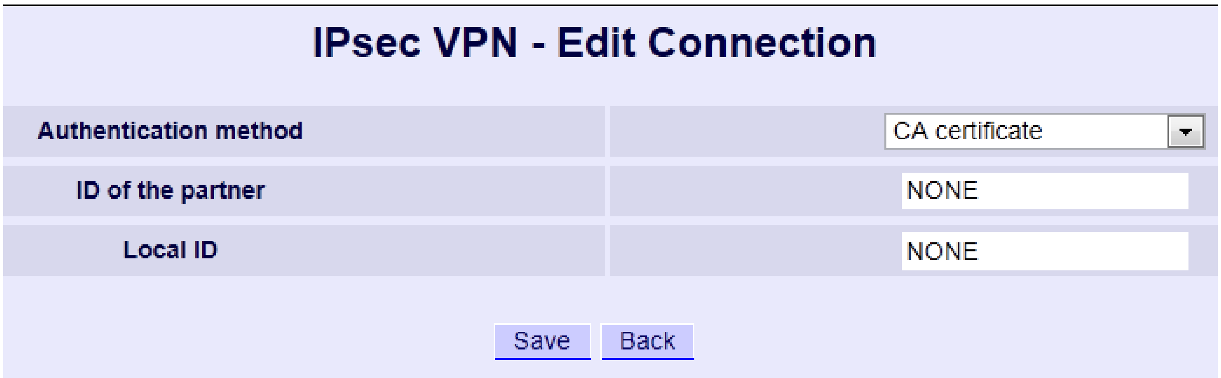
VPN conncetions in roadwarrior mode

Enabled	Name	Connection settings	IKE settings
Yes	Roadwarrior	Edit	Edit

VPN connections in standard mode

Enabled	Name	Connection settings	IKE settings	New

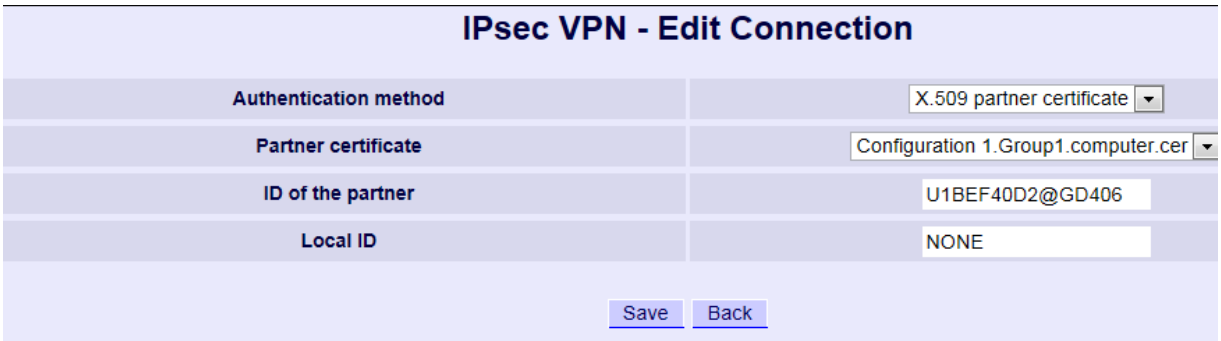
Go back to the “Connections” tab and “Edit” Connection Settings.



IPsec VPN - Edit Connection

Authentication method	CA certificate
ID of the partner	NONE
Local ID	NONE

Step 52 – IPsec VPN edit connections settings



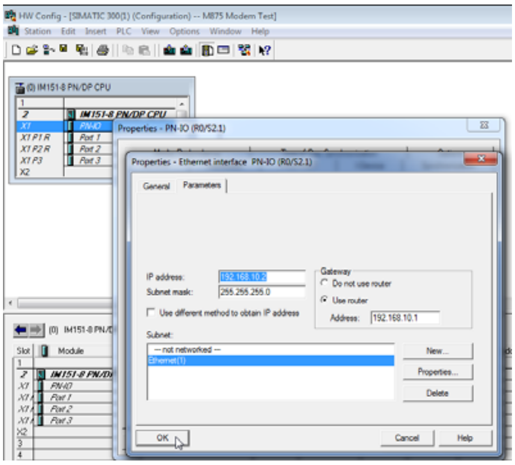
IPsec VPN - Edit Connection

Authentication method	X.509 partner certificate
Partner certificate	Configuration 1.Group1.computer.cer
ID of the partner	U1BEF40D2@GD406
Local ID	NONE

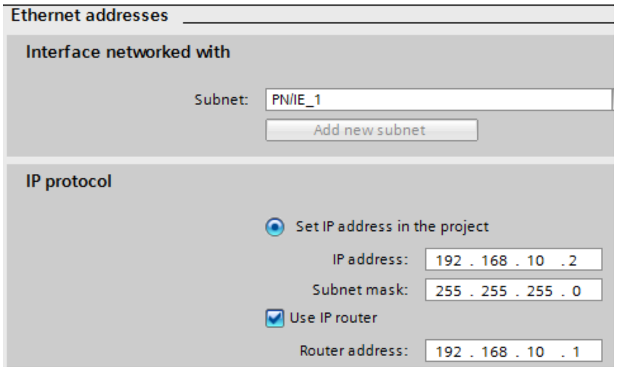
From step 43 we get the following information: enter the data and press “Save”

- IPSec VPN > Connections > VPN Roadwarrior Mode - Edit Settings
- Authentication method: X.509 Remote Certificate
- Remote Certificate: Configuration 1.Group1.computer.cer
- Remote ID: U1BEF40D2@GD406

Step 53 – Step 7 V5.5 project


HW Config - [SIMATIC 300(1) (Configuration) -- M875 Modem Test]
Station Edit Insert PLC View Options Window Help
(0) IM151-8 PN/DP CPU
IM151-8 PN/DP CPU
PN-IO
Port 1
Port 2
Port 3
Properties - PN-IO (R0/S2.1)
Properties - Ethernet interface PN-IO (R0/S2.1)
General
Parameters
New...
Properties...
Delete
OK
Cancel
Help

IP address: 192.168.10.2
Subnet mask: 255.255.255.0
☐ Use different method to obtain IP address
Gateway
○ Do not use router
● Use router
Address: 192.168.10.1
Subnet:
--- not networked ---
Ethernet(1)

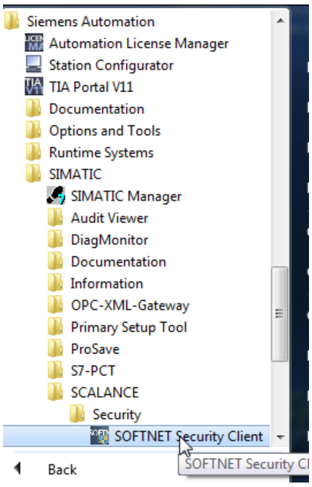


Subnet: PN/IE_1
● Set IP address in the project
IP address: 192 . 168 . 10 . 2
Subnet mask: 255 . 255 . 255 . 0
☑ Use IP router
Router address: 192 . 168 . 10 . 1

Step 7 V5.5 TIA Portal V11

You should now be able to connect an S7 plc to your M875 and go online with it using the Softnet Security Client and Step 7 software. Make sure the PLC configuration sets the IP addrss to an IP address in the range of 192.168.10.x and use router 192.168.10.1. Unplug your pc from the M875 and plug the PLC into the M875.

Step 54 – Start the Softnet Security Client

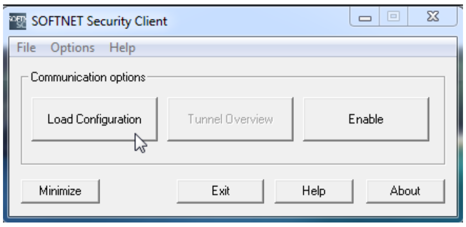


From the Windows "Start Menu" start the "Softnet Security Client"

Copyright ©2013 by SIEMENS page 28 / 34

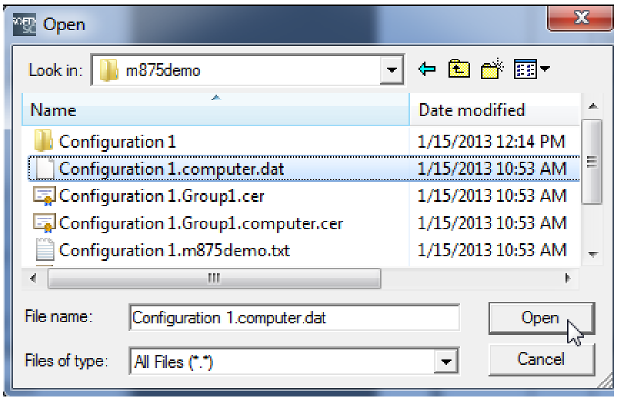
SIMATIC customers have free use of the application tips. These tips are only a general approach to using SIMATIC with various applications. Your specific application may be different. It is your responsibility to use SIMATIC properly in your applications.

Step 55 – Load Configuration



Select “Load Configuration”

Step 56 – Select and open the Configuration file

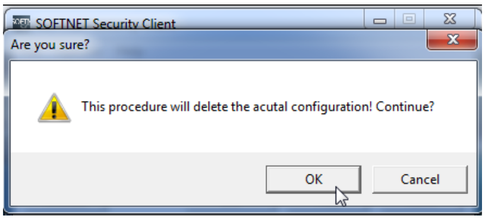


Look in: m875demo

Name	Date modified
Configuration 1	1/15/2013 12:14 PM
Configuration 1.computer.dat	1/15/2013 10:53 AM
Configuration 1.Group1.cer	1/15/2013 10:53 AM
Configuration 1.Group1.computer.cer	1/15/2013 10:53 AM
Configuration 1.m875demo.txt	1/15/2013 10:53 AM

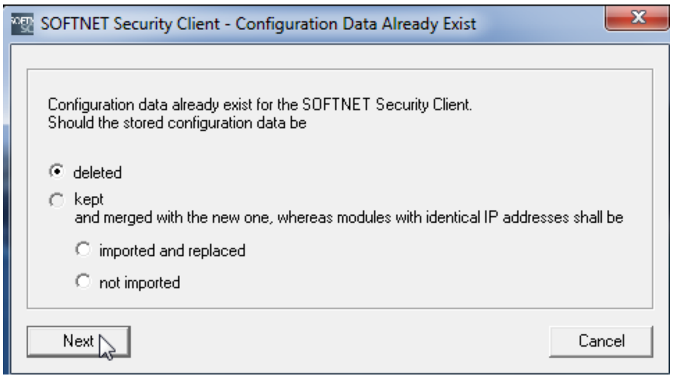
File name: Configuration 1.computer.dat

Files of type: All Files (*.*)



This procedure will delete the acutal configuration! Continue?

You may get this message, just select “OK”



Configuration data already exist for the SOFTNET Security Client.
Should the stored configuration data be

● deleted

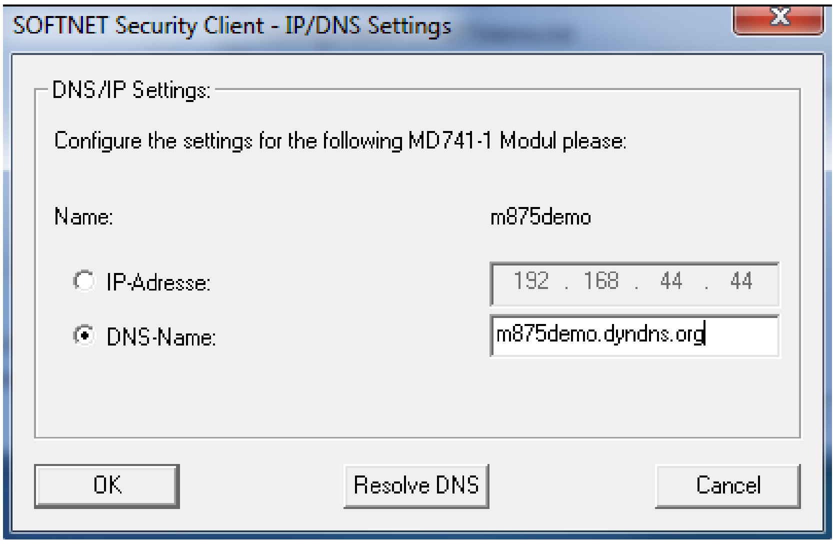
○ kept
and merged with the new one, whereas modules with identical IP addresses shall be

○ imported and replaced

○ not imported

Select “Next” – this is shown if you have loaded a configuration previously.

Step 57 – Select the DNS-Name



SOFTNET Security Client - IP/DNS Settings

DNS/IP Settings:

Configure the settings for the following MD741-1 Modul please:

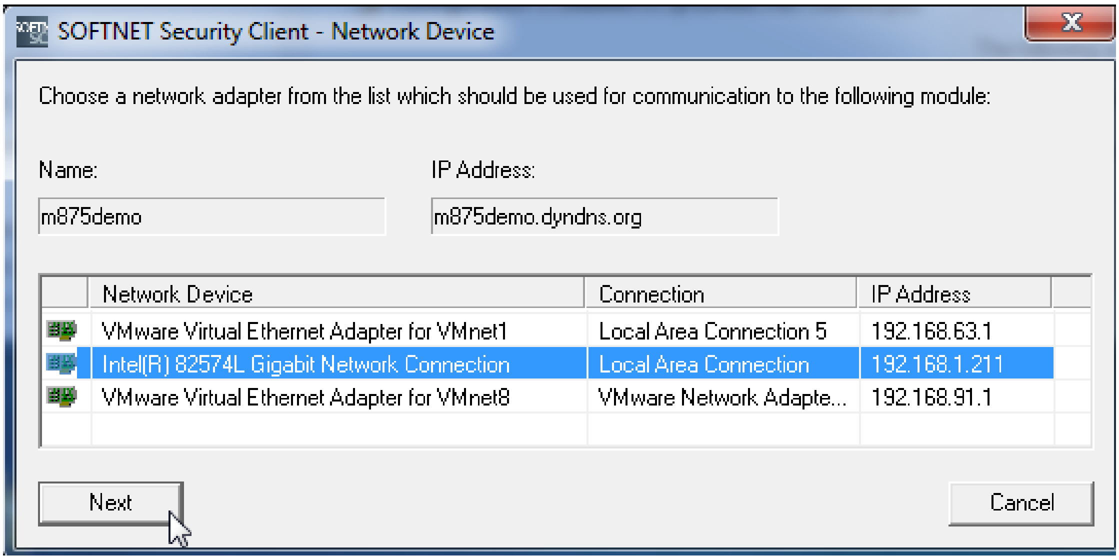
Name: m875demo

○ IP-Adresse: 192 . 168 . 44 . 44

● DNS-Name: m875demo.dyndns.org

If using a static IP address verify that the IP address is correct. For our demo we are using a dynamic address so we use the DNS-Name: - enter the DNS name for your system.

Step 58 – Describe the first topic



SOFTNET Security Client - Network Device

Choose a network adapter from the list which should be used for communication to the following module:

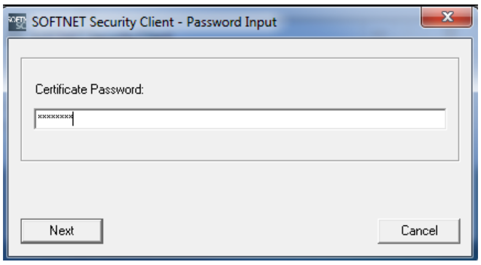
Name: m875demo

IP Address: m875demo.dyndns.org

Network Device	Connection	IP Address
VMware Virtual Ethernet Adapter for VMnet1	Local Area Connection 5	192.168.63.1
Intel(R) 82574L Gigabit Network Connection	Local Area Connection	192.168.1.211
VMware Virtual Ethernet Adapter for VMnet8	VMware Network Adapte...	192.168.91.1

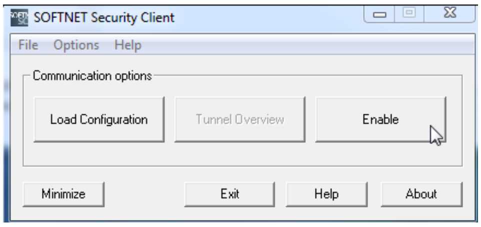
Select the computer's Ethernet adapter that will connect to the internet. Also note that the IP address at the top for the m875demo will either show the fixed IP address of the SIM card or the DNS name that was used.

Step 59 – Enter the Certificate Password

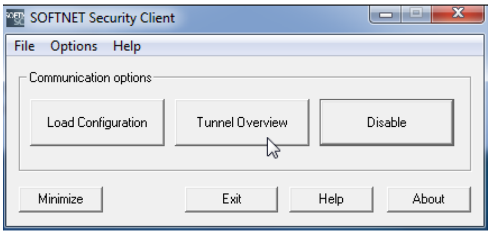

SOFTNET Security Client - Password Input

Certificate Password: ********

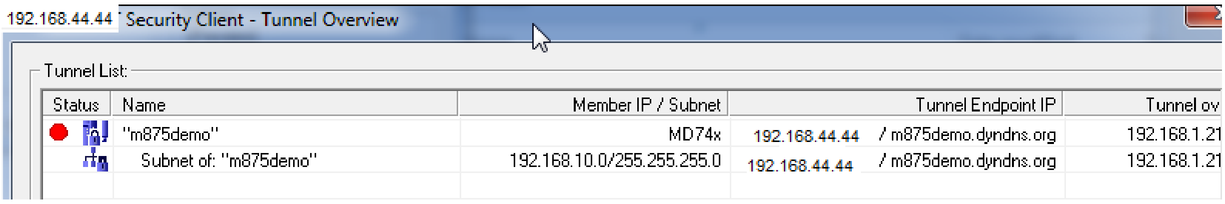
Step 60 – Enable the Tunnel



Step 61 – Tunnel Overview



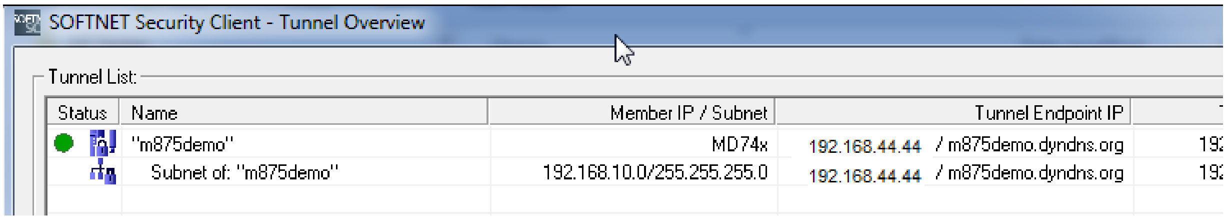
Step 62 – Tunnel status


192.168.44.44 Security Client - Tunnel Overview

Tunnel List:

Status	Name	Member IP / Subnet	Tunnel Endpoint IP	Tunnel ov
●	"m875demo"	MD74x	192.168.44.44 / m875demo.dyndns.org	192.168.1.21
	Subnet of: "m875demo"	192.168.10.0/255.255.255.0	192.168.44.44 / m875demo.dyndns.org	192.168.1.21

If the status is red, the connection has not yet been made.

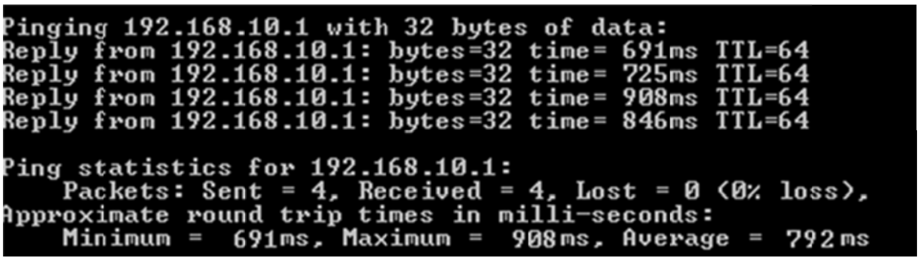

SOFTNET Security Client - Tunnel Overview

Tunnel List:

Status	Name	Member IP / Subnet	Tunnel Endpoint IP	T
●	"m875demo"	MD74x	192.168.44.44 / m875demo.dyndns.org	19:
	Subnet of: "m875demo"	192.168.10.0/255.255.255.0	192.168.44.44 / m875demo.dyndns.org	19:

Green status – tunnel is connected.

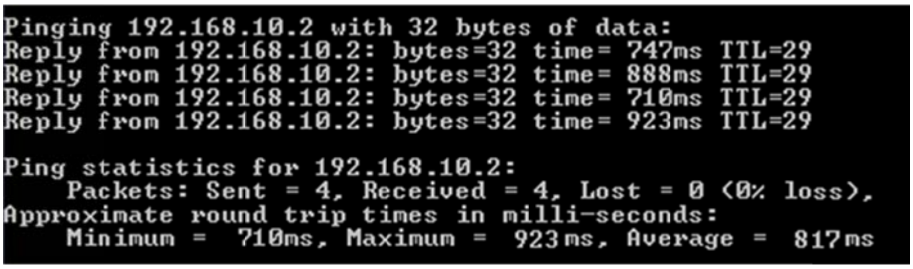
Step 63 – Ping Internal IP address



```
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time= 691ms TTL=64
Reply from 192.168.10.1: bytes=32 time= 725ms TTL=64
Reply from 192.168.10.1: bytes=32 time= 908ms TTL=64
Reply from 192.168.10.1: bytes=32 time= 846ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum =  691ms, Maximum =  908ms, Average =  792ms
```

Ping of the Internal IP address of the M875.

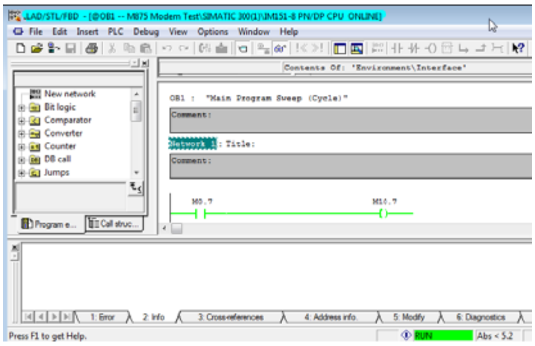
Step 64 – Ping PLC address

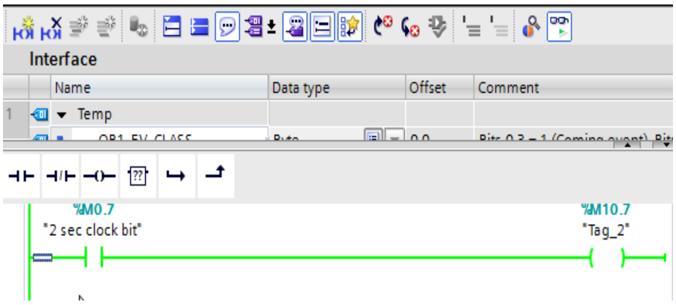


```
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time= 747ms TTL=29
Reply from 192.168.10.2: bytes=32 time= 888ms TTL=29
Reply from 192.168.10.2: bytes=32 time= 710ms TTL=29
Reply from 192.168.10.2: bytes=32 time= 923ms TTL=29

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum =  710ms, Maximum =  923ms, Average =  817ms
```

Ping of PLC address

Step 65 – Online with the PLC

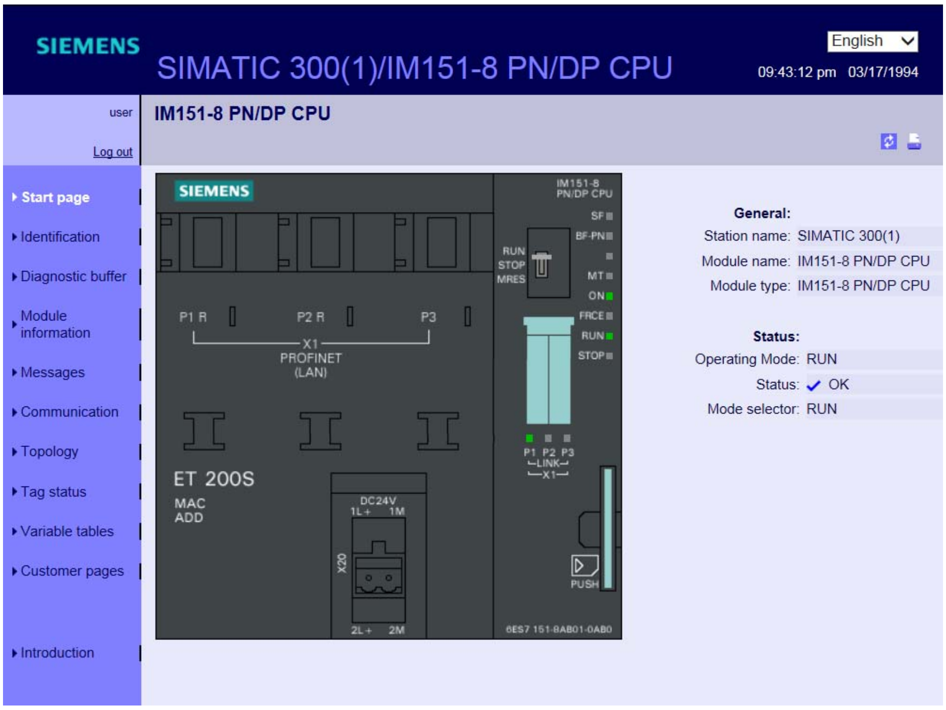




Step 7 V5.5 TIA Portal V11

When using the VPN Tunnel (Softnet Client) no special routing is required from Step7 V5.5 or the TIA Portal V11.

Step 66 – Online with the PLC using the Webserver



SIMATIC 300(1)/IM151-8 PN/DP CPU

09:43:12 pm 03/17/1994

IM151-8 PN/DP CPU

General:

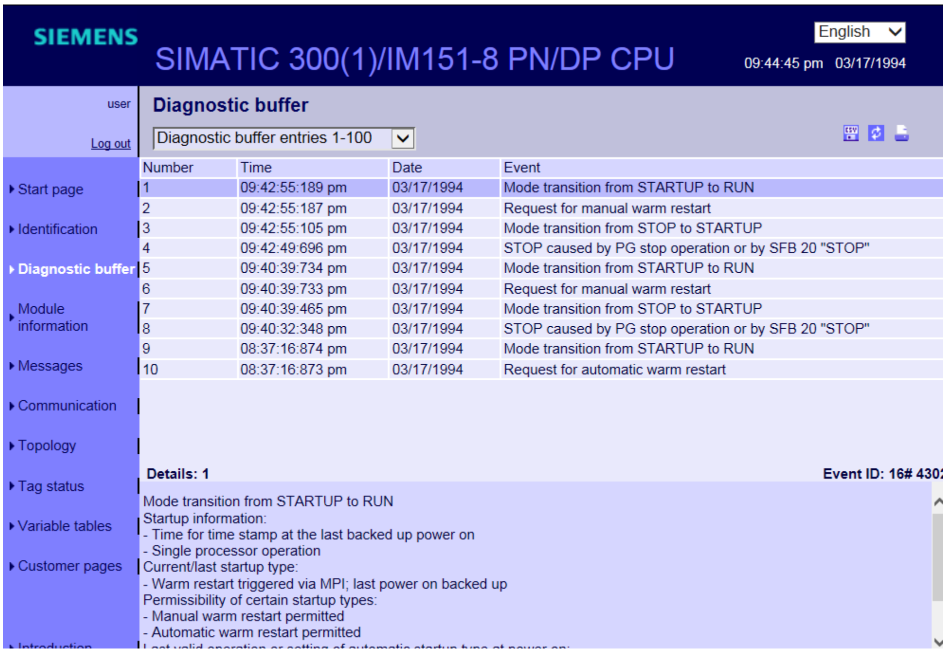
Station name: SIMATIC 300(1)
Module name: IM151-8 PN/DP CPU
Module type: IM151-8 PN/DP CPU

Status:

Operating Mode: RUN
Status: ✓ OK
Mode selector: RUN

Startup page of PLC Webserver using the IP address of the plc – 192.168.10.2 entered into Internet Explorer or Firefox.

Step 67 – Online with the PLC Webserver – Diagnostics Page



SIMATIC 300(1)/IM151-8 PN/DP CPU

09:44:45 pm 03/17/1994

Diagnostic buffer

Diagnostic buffer entries 1-100

Number	Time	Date	Event
1	09:42:55:189 pm	03/17/1994	Mode transition from STARTUP to RUN
2	09:42:55:187 pm	03/17/1994	Request for manual warm restart
3	09:42:55:105 pm	03/17/1994	Mode transition from STOP to STARTUP
4	09:42:49:696 pm	03/17/1994	STOP caused by PG stop operation or by SFB 20 "STOP"
5	09:40:39:734 pm	03/17/1994	Mode transition from STARTUP to RUN
6	09:40:39:733 pm	03/17/1994	Request for manual warm restart
7	09:40:39:465 pm	03/17/1994	Mode transition from STOP to STARTUP
8	09:40:32:348 pm	03/17/1994	STOP caused by PG stop operation or by SFB 20 "STOP"
9	08:37:16:874 pm	03/17/1994	Mode transition from STARTUP to RUN
10	08:37:16:873 pm	03/17/1994	Request for automatic warm restart

Details: 1 **Event ID: 16# 430**

Mode transition from STARTUP to RUN
Startup information:
- Time for time stamp at the last backed up power on
- Single processor operation
Current/last startup type:
- Warm restart triggered via MPI; last power on backed up
Permissibility of certain startup types:
- Manual warm restart permitted
- Automatic warm restart permitted
Last valid operation or setting of automatic startup type at power on:

Diagnostics page of PLC Webserver.

Related Information

Additional Application Notes on M875:

http://support.automation.siemens.com/WW/view/en/24960449

Hardware and Software Considerations

Hardware Used:

- M875 – 6GK5875-0AA10-1AA2
- Antenna - 6NH9860-1AA00
- S7-300 ET200S PLC - 6ES7151-8AB01-0AB0

Software Used:

- Softnet Security Client V4 – 6GK1704-VW04-0AA0
  - With Security Configuration Tool V3 – included with above
- Step 7 Professional 2010 – 6ES7810-5CC11-0YA5
- TIA Portal Professional V11 - 6ES7822-1AA01-0YA5

General Notes

The SIMATIC Application Tips are provided to give users of Siemens' Simatic products some indication as to how, from the view of programming technique, certain tasks can be solved. These instructions do not purport to cover all details or variations in equipment, nor do they provide for every possible contingency. Use of the Simatic Application Tips is free.

Siemens reserves the right to make changes in specifications shown herein or make improvements at any time without notice or obligation. It does not relieve the user of responsibility to use sound practices in application, installation, operation, and maintenance of the equipment purchased. Should a conflict arise between the general information contained in this publication, the contents of drawings or supplementary material, or both, the latter shall take precedence.

Siemens is not liable, for whatever legal reason, for damages or personal injury resulting from the use of the application tips.

All rights reserved. Any form of duplication or distribution, including excerpts, is only permitted with express authorization by SIEMENS.